# DRAFT SF 298

| 1. Report Date (dd-mm-yy)<br>30 April 1996 | 2. Report Type | 3. Dates covered (from... to ) |
|---|---|---|
| 4. Title & subtitle<br>Department of Defense Technical Architecture Framework for Information Management. Volume 1: Overview. Version 3.0 | | 5a. Contract or Grant #<br>5b. Program Element # |
| 6. Author(s) | | 5c. Project #<br>5d. Task #<br>5e. Work Unit # |
| 7. Performing Organization Name & Address | | 8. Performing Organization Report # |
| 9. Sponsoring/Monitoring Agency Name & Address<br>Defense Information Systems Agency<br>Center for Standards<br>10701 Parkridge Blvd<br>Reston, VA 20191 | | 10. Monitor Acronym<br>11. Monitor Report # |
| 12. Distribution/Availability Statement Approved for Public Release: Distribution is Unlimited | | |
| 13. Supplementary Notes | | |
| 14. Abstract<br><br>19970212 103 | | |
| 15. Subject Terms | | |

| 16. Report<br>Unclass | 17. Abstract<br>Unclass | 18. This Page<br>Unclass | 19. Limitation of Abstract | 20. # of Pages | 21. Responsible Person (Name and Telephone #)<br><br>Marilyn McLaughlin<br>(703) 735-3563 |
|---|---|---|---|---|---|

Defense Information Systems Agency
Center for Standards

# DEPARTMENT OF DEFENSE TECHNICAL ARCHITECTURE FRAMEWORK FOR INFORMATION MANAGEMENT

## Volume 1: Overview






Version 3.0

30 April 1996

# FOREWORD:
# ABOUT THIS DOCUMENT

This edition of the Technical Architecture Framework for Information Management (TAFIM) replaces Version 2.0, dated 30 June 1994. Version 3.0 comprises eight volumes, as listed on the following configuration management page.

## TAFIM HARMONIZATION AND ALIGNMENT

This TAFIM version is the result of a review and comment coordination period that began with the release of the 30 September 1995 Version 3.0 Draft. During this coordination period, a number of extremely significant activities were initiated by DoD. As a result, the version of the TAFIM that was valid at the beginning of the coordination period is now "out of step" with the direction and preliminary outcomes of these DoD activities. Work on a complete TAFIM update is underway to reflect the policy, guidance, and recommendations coming from theses activities as they near completion. Each TAFIM volume will be released as it is updated. Specifically, the next TAFIM release will fully reflect decisions stemming from the following:

- The DoD 5000 Series of acquisition policy and procedure documents
- The Joint Technical Architecture (JTA), currently a preliminary draft document under review.
- The C4ISR Integrated Task Force (ITF) recommendations on Operational, Systems, and Technical architectures.

## SUMMARY OF MAJOR CHANGES AND EXPECTED UPDATES

This document, Volume 1 of the TAFIM, contains minor substantive changes from Volume 1 of Version 2.0.

Plans exist to completely revise Volume 1 to transform it to an executive summary reflecting the content of the remainder of the TAFIM. These plans could not be accomplished for Version 3.0 due to funding constraints and the volatility of a number of other TAFIM volumes.

## A NOTE ON VERSION NUMBERING

A version numbering scheme approved by the Architecture Methodology Working Group (AMWG) will control the version numbers applied to all future editions of TAFIM volumes. Version numbers will be applied and incremented as follows:

- This edition of the TAFIM is the official Version 3.0.

- From this point forward, single volumes will be updated and republished as needed. The second digit in the version number will be incremented each time (e.g., Volume 7 Version 3.1). The new version number will be applied only to the volume(s) that are updated at that time. There is no limit to the number of times the second digit can be changed to account for new editions of particular volumes.

- On an infrequent basis (e.g., every two years or more), the entire TAFIM set will be republished at once. Only when all volumes are released simultaneously will the first digit in the version number changed. The next complete version will be designated Version 4.0.

- TAFIM volumes bearing a two-digit version number (e.g., Version 3.0, 3.1, etc.) without the DRAFT designation are final, official versions of the TAFIM. Only the TAFIM program manager can change the two-digit version number on a volume.

- A third digit can be added to the version number as needed to control working drafts, proposed volumes, internal review drafts, and other unofficial releases. The sponsoring organization can append and change this digit as desired.

Certain TAFIM volumes developed for purposes outside the TAFIM may appear under a different title and with a different version number from those specified in the configuration management page. These editions are not official releases of TAFIM volumes.

## DISTRIBUTION

Version 3.0 is available for download from the Defense Information Systems Agency (DISA) Information Technology Standards Information (ITSI) bulletin board system (BBS). Users are welcome to add the TAFIM files to individual organizations' BBSs or file servers to facilitate wider availability.

The final release of Version 3.0 will be made available on the World Wide Web (WWW) shortly after hard-copy publication. DISA is also investigating other electronic distribution approaches to facilitate access to the TAFIM and to enhance its usability.

**TAFIM Document Configuration Management Page**

The latest **authorized versions of the TAFIM** volumes are as follows:

| | | | |
|---|---|---|---|
| Volume 1: | Overview | 3.0 | 30 April 1996 |
| Volume 2: | Technical Reference Model | 3.0 | 30 April 1996 |
| Volume 3: | Architecture Concepts & Design Guidance | 3.0 | 30 April 1996 |
| Volume 4: | DoD SBA Planning Guide | 3.0 | 30 April 1996 |
| Volume 5: | Program Manager's Guide for Open Systems | 3.0 | 30 April 1996 |
| Volume 6: | DoD Goal Security Architecture | 3.0 | 30 April 1996 |
| Volume 7: | Adopted Information Technology Standards | 3.0 | 30 April 1996 |
| Volume 8: | HCI Style Guide | 3.0 | 30 April 1996 |

Working drafts may have been released by volume sponsors for internal coordination purposes. It is not necessary for the general reader to obtain and incorporate these unofficial, working drafts.

*Note: Only those versions listed above as authorized versions represent official editions of the TAFIM.*

This page intentionally left blank.

# CONTENTS

## FIGURES

# 1.0 INTRODUCTION

## 1.1 PURPOSE

This volume presents an overview of the Technical Architecture Framework for Information Management (TAFIM). It relates information technology (IT) and information management (IM) guidance published in the Department of Defense (DoD) directives, instructions, and manuals to the TAFIM.[1]

## 1.2 BACKGROUND

An information system includes support and mission oriented applications, computing platforms, and communications networks. The current DoD information system technical infrastructure consists largely of stovepiped, single-purpose, and inflexible systems that are costly to maintain. These systems reflect a multiplicity of approaches to migrate toward open systems with each one progressing on its own path with limited attention to interoperability.

The evolving DoD enterprise vision for IM emphasizes integration, interoperability, flexibility, and efficiency through the development of a common, multi-purpose, standards-based technical infrastructure. This vision requires a new paradigm for building technical architectures and information systems that improve the effectiveness of functional operations to include their efficiency and use of technology throughout the DoD.

The emerging concepts for warfighting depend upon information being managed as a Department-wide resource. Joint campaigns should fully exploit the "information differential," which is the superior access to and ability to effectively employ information on the strategic, operational, and tactical situation that advanced United States (U.S.) technologies can provide our forces. This information differential requires a seamless interface between the "foxhole" and the support base, between intelligence and operations, and between the DoD and its suppliers. However, today there is no unifying DoD IM technical architecture guidance that can satisfy these goals.

In the absence of DoD-wide IM technical architecture guidance, the Services, Agencies, and Commanders-in-Chief (CINCs) have developed a wide range of architectures to manage and control their technical infrastructures. Reference models, information architectures, communications architectures, mission architectures, and various other architectures are now used to manage the design and development of technical infrastructures and information systems within the Services, Agencies, and CINCs.

---

[1] A list of references is contained in Appendix A. Reference 1 identifies the Executive Level Guidance, which is the source for the IT vision in Section 3 and the IM vision in Appendix C. References 2 through 9 are DoD directives, instructions, and manuals, all of which directly relate to the TAFIM. Reference 10 contains guidance for the preparation of Functional Economic Analyses.

The Technical Reference Model (TRM) for IM was the initial effort to bring commonality and standardization to the technical infrastructure. The TRM addresses the services and standards needed to implement a common technical infrastructure. A single technical architecture framework was needed to integrate these efforts and drive systems design, acquisition, and reuse throughout the DoD.

The single technical architecture framework is the TAFIM. It provides the DoD-wide framework to manage multiple technical architecture initiatives. It is intended to achieve the following results:

- The use of common principles, assumptions, and terminology in the DoD Component (Services, Agencies, and CINCs) technical architectures
- The definition of a single structure for the DoD technical infrastructure components (system components) and how they are managed
- The development of information systems in accordance with common principles to permit DoD-wide integration and interoperability.

## 1.3 TAFIM PURPOSE

The TAFIM provides guidance for the evolution of the DoD technical infrastructure. The TAFIM does not provide a specific system architecture. Rather, it provides the services, standards, design concepts, components, and configurations that can be used to guide the development of technical architectures that meet specific mission requirements.

The TAFIM is independent of mission-specific applications and their associated data. It introduces and promotes interoperability, portability, and scalability of DoD information systems. The TAFIM is an Enterprise Level[2] guide for developing technical architectures that satisfy specific functional requirements. It also provides an organizational level guide and link to the Enterprise Level. To achieve an integrated enterprise, it is assumed that all information systems must interoperate at some time. Therefore, their architects and designers should use the TAFIM as the basis for developing a common target architecture to which systems can migrate, evolve, and interoperate. Over time, interoperability between and among the number of systems will increase, providing users with improved services needed to achieve common functional objectives. To achieve portability, standard interfaces will be developed and implemented. Scalability will be developed in mission applications to accommodate flexibility in the functionality. Proper application of the TAFIM guidance can:

- Promote integration, interoperability, modularity, and flexibility

[2] This should be read as Departmental- or DoD-Level, which are synonymous with Enterprise Level.

- Guide acquisition and reuse
- Speed delivery of information technology and lower its costs.

## 1.4 SCOPE AND APPLICABILITY

The TAFIM applies to information system technical architectures at all DoD organization levels and environments (e.g., tactical, strategic, sustaining base, interfaces to weapons systems) – see Appendix D for further guidance regarding applicability. As Figure 1-1 shows, the TAFIM is intended to guide the development of architectures that satisfy requirements across missions, functional areas, and functional activities [DoD 8020.1-M]. The TAFIM is mandatory for use in DoD. The specific technical architectures for missions and functions will be developed using standard architecture guidance and development methodologies provided by the TAFIM.

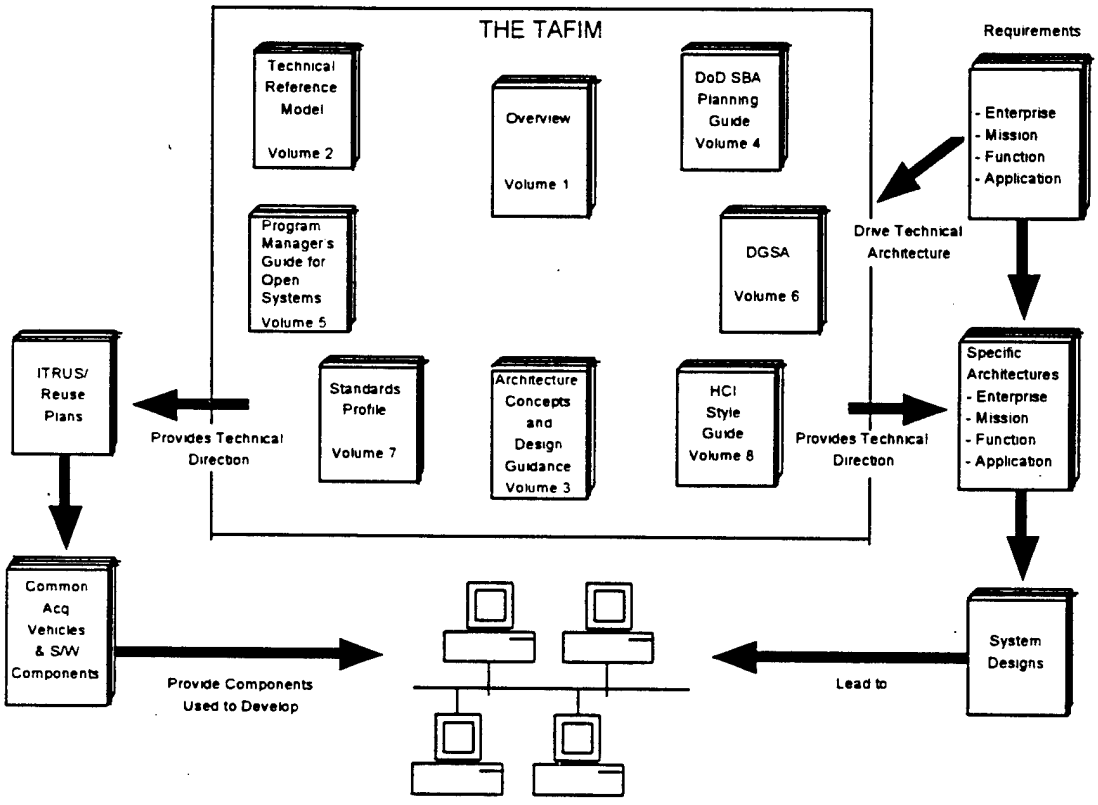


**Figure 1-1. Architecture Implementation Concept**

## 1.5 DOCUMENT ORGANIZATION

Section 2 describes the TAFIM structure and content. Section 3 presents the DoD vision for information technology. Sections 4 and 5 address the information system life cycle and IM integration model, respectively. Appendix A is a list of references. Appendix B defines acronyms and provides a glossary of terms used in the TAFIM. Appendix C provides the DoD vision for IM. Appendix D is the text of three DoD memoranda that provide guidance for using the TAFIM in developing technical architectures. Appendix E provides a format and guidance for proposing changes to this document.

# 2.0 TAFIM DESCRIPTION

## 2.1 INFORMATION SYSTEMS

An information system (IS) consists of mission-specific applications, data, and technical infrastructure architecture consisting of support applications, application platforms, and the external environment including devices such as terminals, printers, and communications networks. Each of these elements has a unique life cycle that requires distinct development and maintenance approaches. For example, data definitions and formats may have a useful life that is many times longer than the mission-specific applications that manipulate and use the data definitions, and the hardware and software that comprise the technical infrastructure architecture may have a life half as long as the mission-specific applications. Each of these elements should be managed according to its life cycle. An information system architecture (ISA) is presented in Figure 2-1 and shows a physical separation of the elements and reflects a mission-specific application software architecture, a data architecture, and a technical infrastructure architecture, which is sometimes referred to as the technical infrastructure architecture.

The data architecture supports standard data elements, data integrity, data availability, shared databases, and the separation of applications and data. The application software architecture supports the development of reusable applications, which are independent of data and the platforms on which they run. The technical infrastructure architecture describes the support applications, computing platforms including the operating system, and external environment needed to provide the connectivity or interoperability for applications and data.

## 2.2 THE TAFIM VOLUMES

The TAFIM provides a set of volumes for guiding the evolution of the DoD's technical architecture, which consists of multiple environments with each environment accommodating one or more ISAs. The TAFIM consists of multiple volumes in various states of development and maturity.

The volumes that constitute Version 3.0 of the TAFIM are listed below.

- Volume 1: *Overview* (this document).
- Volume 2: *Technical Reference Model* provides the conceptual model for information system services and their interfaces.
- Volume 3: *Architecture Concepts and Design Guidance* provides concepts and guidance needed to support the development of technical architectures in the DoD.

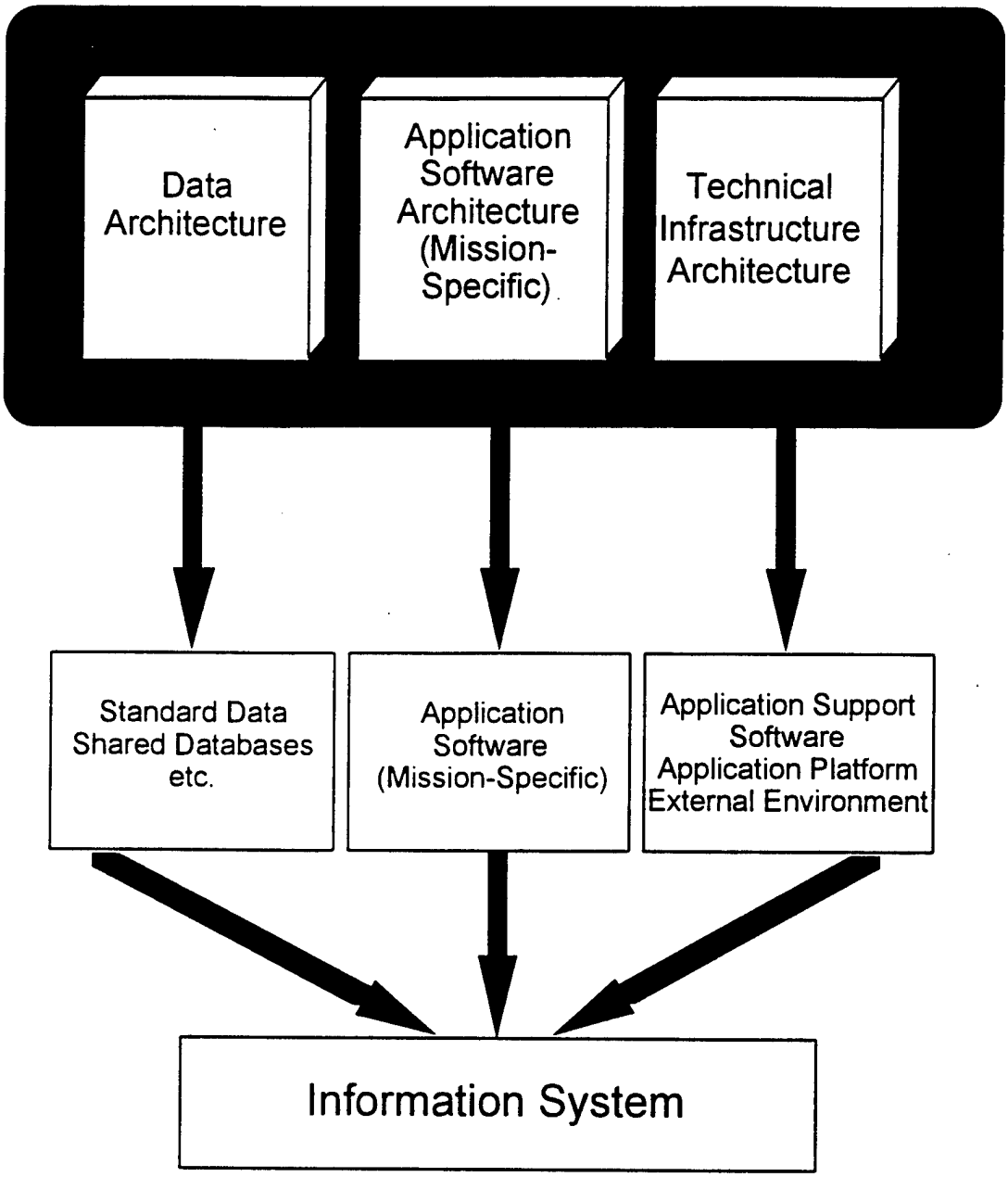


**Figure 2-1. Information Systems Architecture**

- Volume 4: *DoD Standards-Based Architecture Planning Guide* provides a standards-based architecture planning methodology that will help architects, technical integrators, and developers to plan and build information systems that meet mission, functional, and application area requirements. The methodology provides a translation of functional requirements to the selection of services, standards, components, configurations, their phasing, and the acquisition of products that implement them.

- Volume 5: *Program Managers Guide for Open Systems* describes how to use the TAFIM guidance in the acquisition of IT and IM products.

- Volume 6: *DoD Goal Security Architecture* (DGSA) addresses security requirements commonly found within DoD organizations' missions or derived as a result of examining mission threats. Further, the DGSA provides a general statement about a common collection of security services and mechanisms that an information system might offer through its generic components. The DGSA also specifies principles, concepts, functions, and services that target security capabilities to guide system architects in developing their specific architectures. The generic security architecture provides an initial allocation of security services and functions and begins to define the types of components and security mechanisms that are available to implement security services. In addition, examples are provided of how to use the DGSA in developing mission-level technical architectures.

- Volume 7: *Adopted Information Technology Standards* (AITS) is the definitive set of IT standards to be used in DoD. It is intended to guide DoD acquisitions and the migration of legacy systems and, by providing definitive standards, to support broader TAFIM objectives such as interoperability, reduced life-cycle costs, and security.

- Volume 8: *DoD Human Computer Interface (HCI) Style Guide* provides a common framework for HCI design and implementation.

This page intentionally left blank.

# 3.0 THE VISION FOR DOD INFORMATION TECHNOLOGY

This section focuses on the vision [Executive Level Guidance (ELG)] for DoD information technology. It is part of the total DoD guidance for planning, developing, and operating the DoD's information systems. Implementing state-of-the-art information technology provides for improved information management. The TAFIM furthers this concept. It also supports the information management vision, described in Appendix C. They both relate to the DoD information systems technical infrastructure.

Information technology is integral to providing efficient and effective functional information management processes and practices across the DoD. It is recognized as a force multiplier during peacetime, transition to war, and war. The implementation of information technological principles and products into all aspects of DoD operations means that effective military capabilities can be maintained within smaller defense budgets.

## 3.1 TECHNOLOGY

Off-the-shelf information technology is becoming more flexible and powerful. Within DoD, this information technology eventually will extend from the foxhole to the office, in fixed and mobile locations, across the full spectrum of peace, transition to war, and war. It will be ubiquitous and integral to all DoD operations and user tasks.

The information technology will make possible capabilities that encompass all composite objects consisting of different types of related temporal and logical content that can be entered, accessed, manipulated, and displayed at every workstation as an integral part of each job. Workstation platforms and other user devices that become available in the early twenty-first century are expected to be many times more powerful than the machines of the early 1990s. Workstations will adhere to a full suite of Federal, national, and international standards that have been adopted by the DoD. Because platforms adhere to a common set of interface standards, it will be possible to configure software across a distributed environment and tailor the software to support specific functional processes. The ubiquity of standard low-cost platforms, coupled with rapid and responsive software development, will enable effective implementation of continuous functional process improvements.

## 3.2 PRODUCT AVAILABILITY

Commercial software products, supplemented (when necessary) by Government-developed reusable components, will provide DoD's IM system developers with powerful tools to enhance productivity and decision making. The accumulated experience of DoD personnel will be preserved through standard databases that are portable across platforms, locations, applications, and assignments. Users also will be provided with the tools to tailor screens, menus, and applications so that they can be more productive, innovative, and effective in the performance of

assigned duties. Policies, procedures, standards, and controls will govern this individual capability, ensuring that its use is consistent with military doctrine and mission IM standards.

## 3.3 ROUTINE OPERATIONS

DoD information systems and their associated improved processes will perform many of the current individual manual and routine operations, allowing individuals to perform value-added work. With such capabilities, individuals and groups may dynamically configure information resources (e.g., data, processing resources). In effect, users will set up their own virtual operations/work spaces and use them to get the immediate task accomplished. When a task is finished, the resources will be returned to a common pool, and new tasks will begin. This reconfigurable information resources model enables developers to create an environment that supports routine work as well as serving dynamic battle situations with technology that transitions smoothly from peace to war.

## 3.4 OPEN SYSTEMS ENVIRONMENT

DoD is fully committed to implementing an open systems environment (OSE). This environment will enable information systems to be developed, operated, and maintained independent of application-specific technical solutions or vendor products. DoD is establishing a standards-based framework for defining technical architectures to provide interoperability, portability, and scalability. System attributes such as performance, response time, and availability, which are not part of the open system, will be separately defined within the requirements of the functionality as implemented in each Automated Information System (AIS). The TAFIM uses Federal and national standards adopted by industry, and international standards accepted worldwide by U.S. allies. The guidelines will show technical managers and developers at all levels of the DoD how to create profiles of standards to meet specific mission-area architecture needs. Also, the guidelines will provide transition strategies on how to evolve baselines and legacy systems to the target open environment. When developing information systems, the DoD Components and subordinate commands will follow the guidelines and apply the standards recommended by TAFIM. This will enable all functions to work together, and all systems to benefit from the efficiencies made possible through the shared part of the DoD infrastructure.

DoD has and will continue to play a leadership role in the development of standards that contribute to open systems by working in concert with national, international, and industry bodies. DoD is beginning to work with vendors to ensure they incorporate standards recommended by TAFIM, capabilities, and features in their products for use in DoD systems.

## 3.5 DATA AND INFORMATION SECURITY

Security of vital DoD information resources will be achieved through a common approach to integrated policy, architecture, and engineering using the DGSA concepts in conjunction with other DoD guidance. Security architectures will satisfy mission-area security policies and align

with TAFIM-recommended standards that address open systems. The protection of information and system assets will be part of the total security requirement for automated services. DoD systems support information processing under arbitrarily complex security policies, including those involving support of multiple categories of sensitive classified and unclassified information. The systems will be sufficiently protected to allow distributed processing among multiple hosts on multiple networks in accordance with open system architectures. They support information processing among users employing resources with various types of security protection, including users of non-secure resources if a particular mission so dictates. The DoD information systems will be sufficiently protected to allow connectivity via common carrier (public) communication systems.

The DGSA will allow different mission-area information systems to exchange information in a secure manner yet ensure the integrity, confidentiality, availability, and authenticity of enterprise databases and resources.

## 3.6 THE DOD INFORMATION UTILITY

The DoD will operate an information utility that users can access worldwide to obtain needed information services. The information utility will be transparent and will deliver a full spectrum of quality services, where and when needed, tailored to the job, affordably priced to match alternative sources, when appropriate and available. This environment will be managed from a DoD-wide perspective to achieve a balance of centralized, local, and individual capabilities. All DoD shared information resources, both owned and leased, form a global network that will be centrally managed as part of the overall systems and networks of the Defense Information Infrastructure (DII) across the various environments, including:

- Central processing centers that house the master copies of corporate databases and perform large-scale production jobs
- Fixed site installations and mobile facilities where application processing occurs, where networks and systems are managed, and where the data are captured and stored for local use
- The personal computing environments that enable individuals to manage their information resources.

## 3.7 SHARED DATABASES

Shared databases will be established, centrally managed, and controlled to ensure the integrity of the information resource for the entire DoD. Rules and mechanisms will be put in place to allow individuals to make individual use of data while maintaining the data standards established for all users, including appropriate security controls. Data that crosses DoD Component or functional boundaries will be kept in shared databases and accessed over the common-user global network. These corporate-type databases will be governed by consistent data models, centrally managed, logically integrated, and physically distributed worldwide, with automated

backup and recovery. The DGSA is an integral part of the TAFIM. It specifies security principles and targets security capabilities that will guide system architects in creating specific architectures that will meet mission security policies.

## 3.8 BACKBONE NETWORK

The DoD will establish, operate, and centrally manage a Defense Information System Network (DISN) as part of the DII that will evolve to make use of highly available, ubiquitous, global, commercial communications networks for the vast majority of the DoD communications needs. These networks will feature the cost savings of bandwidth-on-demand service and integrated services for voice, data, and video applications. The DISN will provide value-added services for secure and non-secure directories, conferencing, and databases. The DISN will also provide backbone connectivity between users who require the special protection of complete traffic flow security.

This backbone connectivity will eventually extend to desktops and mobile devices. It will be survivable, robust, and centrally managed to optimize the use of resources, availability, and performance. A security architecture, using DGSA concepts, and new procedures will allow different functional communities to exchange information easily while maintaining the integrity of their mission areas.

## 3.9 STREAMLINED LIFE CYCLE

A streamlined life cycle will be used to compress the time needed to deliver new capabilities to the field and to reduce total life-cycle costs. The process will emphasize the use of powerful and integrated computer-assisted methodologies and tools such as the shared utility services, reuse of software components, refurbishment and replenishment of hardware acquired as a commodity item, building-block construction of systems, use of products meeting the DoD architecture guidelines and standards, and improved technical management. Ad hoc system development efforts will not be permitted. System developments will be organized and engineered to be repeatable and reliable so as to achieve quality, efficient, and effective rapid production.

## 3.10 MODELING AND PROTOTYPING

Data modeling is becoming mature. It will be fully integrated with process modeling in a common DoD-wide approach. Powerful and integrated computer-assisted development and maintenance environments will rapidly capture process models, data models, and other requirements and transform them into applications and databases that adhere to DoD standards for data elements and software. Rapid prototyping will be a built-in aspect of the systems development cycle, so that incremental changes that support improved business processes can be accomplished in days and weeks rather than months and years.

## 3.11 STREAMLINED ACQUISITION

A streamlined acquisition process will be functioning that ensures the implementation of the DoD information system infrastructure can be achieved on schedule and within budget. Compliant components will be available from "one-stop shopping" technology "stores" when they are needed. Hardware and most generic software components (e.g., database management systems, electronic mail (E-mail) packages) will be acquired as products that serve mission-area applications, which embody specific business rules and user interactions.

Acquisition lead-times will be shortened to avail the DoD of new cost-effective technology's best suite to improve functional processes. Open system standards will expedite the acquisition process by reducing the time and cost of migrating to improved environments. Innovative mechanisms, such as hardware leasing, will be in place to acquire a full spectrum of information products and services at the best cost value to the Government. Products may be procured as new, reused, or refurbished in a cost-effective manner. These improvements will be supported by test and evaluation (T&E) methodologies that are being overhauled to support the rapid acquisition of information systems.

## 3.12 PERFORMANCE

The DoD technical infrastructure will be founded on a baseline of standard configurations that will provide the required performance within cost. Measures of effectiveness (MOE) will be used to evaluate how well the infrastructure is supporting the functional users. The application of MOEs (including benchmarking against industry best practices) will assure DoD managers that the infrastructure technology is effective and efficient and that the service provided compares favorably with the commercial support provided to the public sector. IT will be managed, in the same way as other IM activities are managed, to enable continual improvement. Although IM has to be managed, in an authoritarian organization like DoD, use of open systems assumes that the end users (action officers, not clerks) have a wide range of tools, capabilities, and applications with appropriate access to enterprise data. Once this is granted, the users will be empowered and authorized to utilize this information technology. The end use of the system should not be managed – rather, the effectiveness of providing that environment to the users should be managed.

## 3.13 EDUCATION AND TRAINING

Education and training of the DoD IM community in new methods, tools, and practices will be centrally managed. The goal will be to create technically literate users, who can obtain the maximum benefits from the new technologies. There will be a renewed emphasis on enhancing individual skills, productivity, professional growth, and job satisfaction. This emphasis recognizes that DoD personnel are the most important DoD resource.

This page intentionally left blank.

# 4.0 INFORMATION SYSTEM LIFE-CYCLE SUPPORT

## 4.1 LIFE-CYCLE MANAGEMENT

The TAFIM supports life-cycle management (LCM) as published in DoD guidance directives [DoD Directive (DoDD) 8120.1 and DoD Instruction (DoDI) 8120.2]. It also supports the LCM method of reporting system development progress to decision makers and specifically addresses those efforts that take place in the development phase of new information systems or in the update to existing information systems.

## 4.2 INFORMATION SYSTEMS DEVELOPMENT

The TAFIM supports evolutionary, incremental, and concurrent development methods that contribute to reducing the time it takes to field new or revised capabilities. Whatever method is selected, it is documented in life cycle documentation presented to decision makers for approval. Figure 4-1 presents a method where requirements are identified as input to the development and operation of an information system.

The figure relates TAFIM guidance, development aids, tools, and products to the development cycle. The developer should take every advantage of the TAFIM guidance and of available development tools and aids. Development support includes prototyping, standardized data and database sharing, procuring commercial-off-the-shelf (COTS) products, reusing common applications software, implementing common-use infrastructure services (computer and communications utility), and using integrated computer-aided software engineering (I-CASE) tools. The products and services are standards-based and architecturally driven. The use of standards and common technical architectures will reduce the likelihood that stove-pipe systems will be developed. This should result in system components that are interoperable, compatible, flexible, and operationally efficient, even though they are acquired and configured by different executive agents.

Within common architectures, applications, data, and infrastructures must be managed according to their separate life cycles. To make this approach work, the various support tools and mechanisms for designing, prototyping, developing, acquiring, integrating, testing, fielding, and operating information systems must adhere to the common architecture principles, guidelines, and standards. Their implementation should employ innovative methods, tailored to meet the situation associated with the requirements. The blocks shown in Figure 4-1 are briefly discussed in the following subsections.

### 4.2.1 Requirements Definition

The Enterprise Model described in DoD 8020.1-M provides the framework for developing integrated process and data models for specific functional activities in the DoD. Together, these

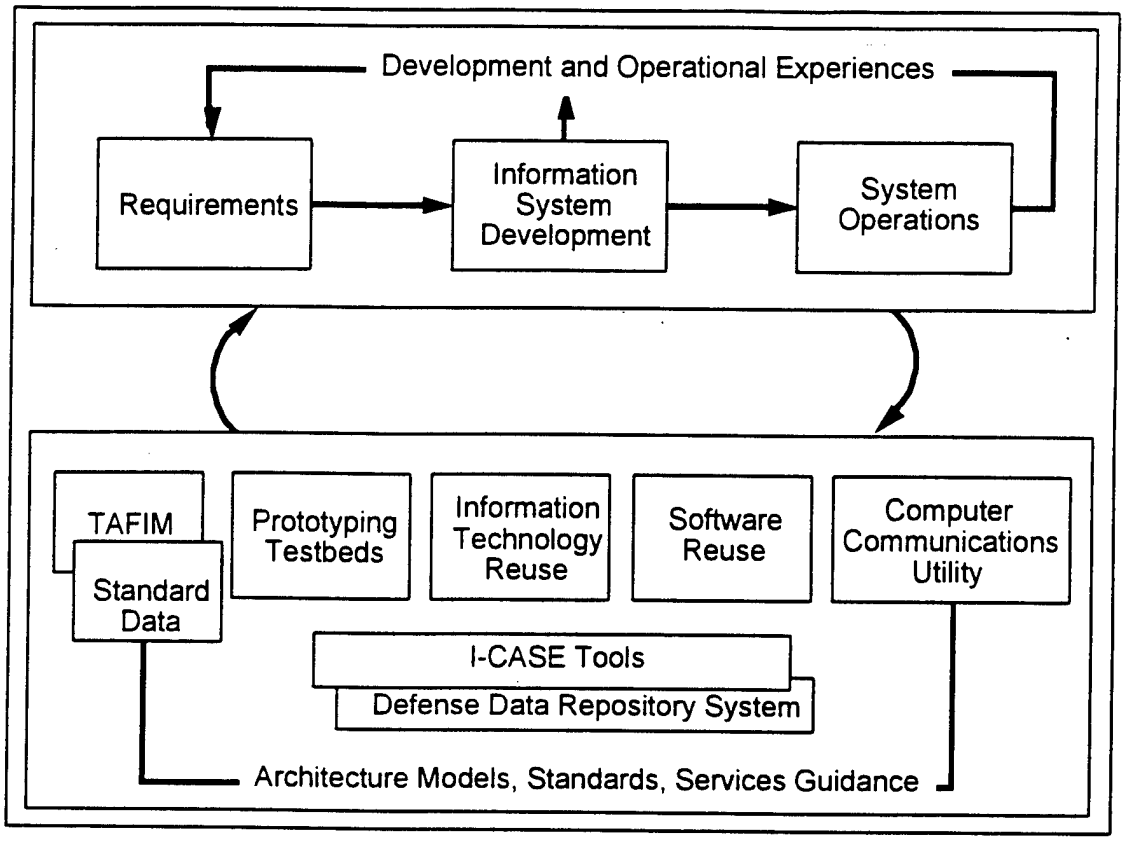


**Figure 4-1. Information Systems Life-Cycle Support**

models specify the functional user (logical) requirements for an information system. In addition to addressing the foregoing, DoD 8020.1-M addresses the DoD Data Administration Strategic Plan (DASP) and other DoD IM documents. The model requirements provide input for developing the technical architecture addressed in the TAFIM. The requirements are established using a DoD standard methodology, described in Chapter 8, DoD 8020.1-M. This or other methodologies provide the requirements input for information system development.

### 4.2.2 Information Systems Development

The TAFIM provides guidance to architects and designers on the selection of compatible configurations of standards, services, and components that can be implemented through common-use acquisitions, DoD software reuse libraries, and shared utility services (e.g., a global network). Development activities define an ISA that is based on functional requirements and consists of the data architecture, application architecture, and technical architecture. The technical architecture guidance is provided by the TAFIM. The data and mission application software architectures [DoDDs 4630.5, 8000.1, 8120.1, 8320.1] are developed by mission or function. Together they require integration into the overall infrastructure.

To assist the development activity, the TAFIM includes a reference model and services, a tailorable standards profile, architecture concepts, and design guidance. Information system development efforts include rapid design and prototyping. These efforts include the use of corporate data, reusable software, and infrastructure "building blocks" from various DoD IM initiatives that are being documented in the TAFIM. Detailed engineering guidance, particularly for migrating from or interfacing to legacy environments, is outside the current scope of the TAFIM.

TAFIM Volume 4, *DoD Standards-Based Architecture Planning Guide*, provides a standards-based architecture development methodology. In general, this methodology starts with the functional models and requirements and includes evaluating the baseline for deficiencies and opportunities, selecting a target or open architecture, and identifying migration paths and actions to evolve from the baseline to the target architecture. This process involves integrating the data architecture, mission application architecture, and technical architecture into a total ISA.

In support of the TAFIM, the Defense Data Repository System (DDRS) will be integrated with I-CASE, the IDEF repository, and the software reuse libraries. The DoD Software Reuse Program will provide software components that implement standards recommended by TAFIM and its guidance. An example would be software modules that use standard application program interfaces (APIs). Applications developed by specific functional communities will be put in central libraries and made available to development activities. The concept allows for lead development activities that develop integrated sets of application software for functional domains, including shared system software. Software components developed according to Software Reuse Program standards and design guidelines must be consistent with the TAFIM to promote reuse, portability, and interoperability of systems in the DoD. I-CASE tools and integrated software development methods will be selected and configured to support the TAFIM. For example, I-CASE tools will generate code that uses the APIs specified in the TAFIM.

Prototyping environments will adhere to the TAFIM guidelines and standards and use information technology reuse (ITRUS) components, DoD software reuse products, and I-CASE prototyping tools to the maximum extent possible. This will facilitate rapid prototyping of applications and databases that can be validated by users and easily transitioned into production environments.

### 4.2.3 System Operations

Information systems will be operated in the global computer and communications utility environment that adheres to standards recommended by TAFIM and its guidelines. This will promote portability, survivability, flexibility, and interoperability for all DoD information systems. Centrally managed processing centers, global networks, sustaining base installations, and tactical environments will be developed using the basic approach outlined above. Databases and applications that use the standards recommended by TAFIM and its design features will become largely independent of where they are hosted. They will be easily portable across the

infrastructure environment, allowing efficient resource utilization, backup, and least-cost utility service to the customer.

## 4.3 INFORMATION SYSTEMS EVOLUTION

The TAFIM provides the basis for interoperability of information systems by defining common services, standards, and configurations for the DoD technical infrastructure (i.e., support applications, application platforms, and communications networks). New DoD information systems will achieve interoperability by being built in conformance with an ISA based on the design guidance and standards set forth in the TAFIM. Interoperability of existing systems will be increased by evolving them to ISAs that are consistent with the TAFIM.

To evolve existing systems, functional and technical teams assess existing systems as part of the mission-area or DoD Component-wide strategic planning process. These teams determine the degree that the existing systems are in compliance with functional requirements and provide required services. They also assess how well existing systems meet standards that accommodate open systems. These teams determine and evaluate the cost, time, and risk required to evolve existing systems to the goal architecture. These assessments can be an input to the Functional Economic Analysis (FEA) [DoD Corporate Information Management (CIM)] that is a consideration in the process of selecting existing systems for migration or authorizing a new start AIS.

The rate at which different system baselines converge to the open systems architecture is governed by many factors, including the need to select migration systems and to develop them to a common open architecture in the DoD, and in so doing, implement functional process improvements. Many systems are currently implemented in unique or proprietary environments from which it is difficult to evolve. Figure 4-2 shows how migration systems and other systems will go through several phases in their convergence to an open systems target architecture during the 1990s and beyond.

The first phase is constrained by the need to continue some legacy systems while selecting others as standard migration systems. Therefore, near-term target architectures will continue to have legacy and proprietary elements that must interface with migration systems as they evolve to open systems elements. Once the target baseline is achieved, there will be greater opportunities to satisfy functional process improvement support needs with open systems solutions. Finally, systems can be planned so as to evolve to standards that accommodate open systems.

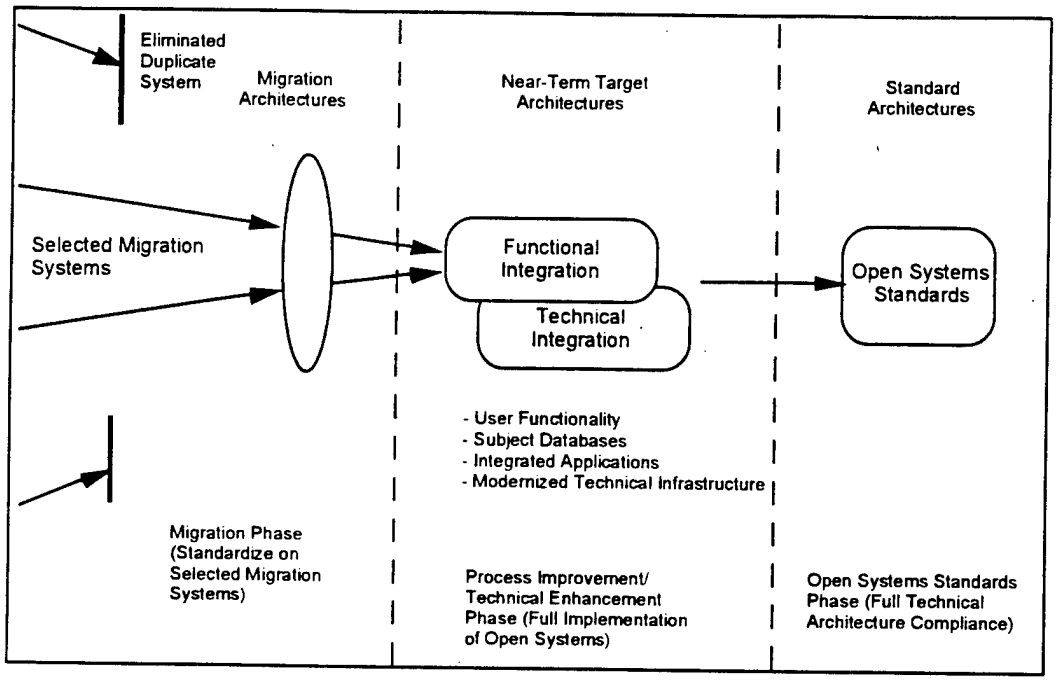


**Figure 4-2. Phased Convergence To DoD Open Systems Architecture**

This page intentionally left blank.

# 5.0 INFORMATION MANAGEMENT INTEGRATION MODEL

## 5.1 INTRODUCTION

Functional and technical integration of user requirements presents significant potential for cost savings and system flexibility. Since, user requirements differ in a number of ways, their integration can mean that the user will not require multiple products or services to meet these multiple needs.

## 5.2 OBJECTIVE

The objective of integration [DoD 4630.5 and DoDI 4630.8] is to:

- Achieve or improve system interoperability
- Achieve compliance with international, national, and DoD open systems standards
- Provide users a single common interface
- Achieve portability and flexibility.

## 5.3 DESCRIPTION OF THE INTEGRATION MODEL

Integrating functional and technical requirements of DoD information systems can be portrayed using the DoD IM integration model shown in Figure 5-1. It represents a perspective for defining boundaries for potential integration pay-off within DoD IM activities from a DoD-wide view. Further, it can assist integrators in defining what is to be integrated in order to correctly proceed with the task. Functional and technical integration requirements must be addressed both at the vertical boundaries within a level and the horizontal boundaries between the levels of the model.

## 5.4 TYPES AND LEVELS OF INTEGRATION

Integration can occur within or between the levels of the model but the requirements for the type of integration must still be defined. To gather these detailed requirements, significant research and analysis efforts may be required to gain a full understanding of the integration task. Integration should result in interoperability and efficiency, effectiveness, optimization, resource savings, or other benefits. Integration will be viewed from at least one of the following perspectives:

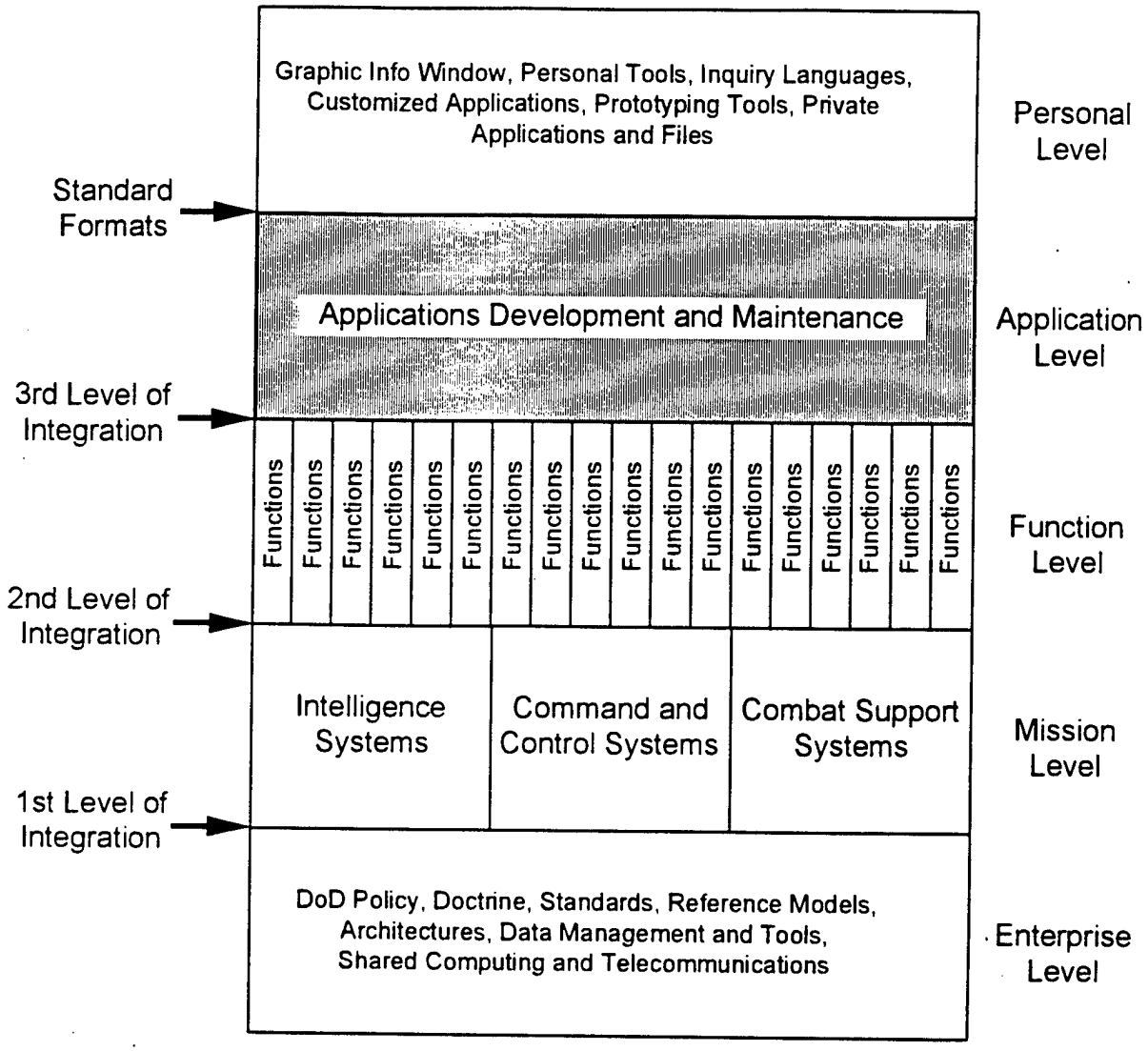


**Figure 5-1. DoD IM Integration Model**

- Functional integration: Functional integration generally involves collapsing two or more software modules that have similar functionality into a single new software module or involves relating two or more software modules with dissimilar functionality through a common database.

- Technical integration: Technical integration generally involves issues of compatibility and connectivity for interoperability of hardware and could involve software where relationships are involved (e. g., conversion between protocols).

### 5.4.1 The Enterprise Level

Level 1 is the Enterprise (or DoD-wide) Level. This level consists of integrating processes and procedures that are either manual or automated for all mission areas and their functions. Level 1 encompasses information management elements that are mandatory across the DoD. It includes IT and IM policy, procedures, standards, and doctrine that are established by the DoD or the Joint Chiefs of Staff (JCS). This level also includes standard IT capabilities such as technical and data standards, reference models and architectures, methods and tools, and shared computing and communications services. The integration and coordination of enterprise-level IT tasks support broad DoD policy and doctrine and are the responsibility of the Deputy Assistant Secretary of Defense (DASD) for IM. At this level, broad integration guidance and strategies for DoD information systems are established by the Defense Information Systems Agency (DISA) Joint Interoperability and Engineering Organization (JIEO).

The Enterprise Level is the foundation for standardizing technologies and services across the DoD. At this level, DISA develops common architectures, designs, and centrally manages the computer and communications utility. This utility is a global network that includes central processing resources, interoperable design activities, a DDRS and IDEF repository, shared databases, standards, central acquisition, security based on the DGSA, education and training, and other global and local common-use information technology services. The TAFIM is developed at this level to guide the development of the DoD technical architecture of this utility, to guide its use at other levels, and to promote total integration, interoperability, effectiveness, and efficiency including security of the DoD technical infrastructure through implementing DGSA concepts. When the TAFIM guidance and standards profile (and other DoD-wide architecture guidance such as the DGSA) are applied at other integration levels, DISA will review the resulting architecture products for conformance. The DGSA is a generic goal architecture that is designed as an integral part of the TAFIM guidance for the Enterprise Level.

### 5.4.2 The Mission Level

Level 2, the Mission Level, is composed of major DoD mission areas that are supported by systems for the mission areas such as Command and Control (C2) Systems, Intelligence Systems, and Combat Support Systems. (Combat support systems, formerly called business systems, include all systems that act as supporting elements for DoD.) At this level, areas of specialization and functional focus emerge, and mandatory DoD-wide technical requirements and capabilities are supplemented with mission-area specific requirements and capabilities. Strategy and planning for this level are developed under the direction of the DoD Principal Staff Assistants (PSA) and their appointed Functional Activity Program Managers (FAPMs) [DoD 8020.1-M].

At this level, DISA manages the integration of information systems functionality and technology within and across mission areas to achieve common major end-to-end functionality for command and control, intelligence, and business systems support. DISA tailors DoD-wide architectures, strategies, and plans for common use in networks, shared processing, and central design activities to satisfy mission-area requirements. For example, the TAFIM encourages tailoring to

fit mission-area specific requirements of warfighters, intelligence analysts, and resource managers. JIEO prepares broad information system integration guidance for the development of information system integration strategies at the function level.

### 5.4.3 The Function Level

Level 3, the Function Level, includes multiple activities and processes of the DoD [DoD 8020.1-M]. At this level strategy and plans for these activities and processes are developed under the direction of PSAs or Principal Deputy Assistant Secretaries of Defense and their appointed FAPMs. Architectures are defined for the "to-be" functional operational practices and processes in accordance with DoD 8020.1-M and Change 1. Data models, activity models, and data architectures are developed to support simplified, streamlined, and improved practices and processes. Information system strategies and plans are developed that identify functional and technical requirements, priorities, schedules, and constraints for evolving information system baselines to the target information systems based on common architectures. In accordance with DoD IM policies and guidelines, DoD-wide and mission-area architectures are tailored to fit specific requirements, priorities, and constraints associated with unique functionality. The DoD Data Administrator (DA) and other elements of DISA work with the FAPM to ensure that functional data and information system strategies and plans conform to this guidance. They also review the Function Level architectures for conformance with DoD and mission-area architectures.

### 5.4.4 The Application Level

Level 4, the Application Level, includes the development, maintenance, and operation of information systems. In the integration concept each mission-area application can support a process, an activity, or a complete function. The application may execute on hardware bases that are distributed, shared, or dedicated. At this level, central design activities and data processing installations apply improved methods, tools, products, and services available through the activities of the Enterprise, Mission, and Function levels for design and development. Information systems are implemented by technical development activities in accordance with strategies and plans prepared at the function level.

### 5.4.5 The Personal Level

Level 5, the Personal Level, includes personal productivity tools and individual tailoring of automated capabilities for the end users. The tailoring must conform to guidelines and procedures that ensure the integrity of shared resources as well as effective operations in peacetime, transition to war, and war.

## 5.5 VIEWS OF THE INTEGRATION MODEL

The IM process is simultaneously a bottom-up and top-down process that is harmonized by new processes and procedures and technical integration support. As the cross-functional integration process takes hold, there will be a greater use of common architectures and "building blocks"

managed at the enterprise and mission levels. Initially, however, process models, data models, standards, and information system architectures will be generated largely from a functional area and functional activity perspective to achieve immediate corporate IM objectives (e.g., migration toward system standardization). This reduces the need to develop new data, applications, and technical infrastructures. The two views are discussed below.

### 5.5.1 The Bottom-Up View

The bottom-up view is the foundation for each upper level of the integration model, which rests on a shared foundation of common policies, processes, procedures, methods, tools, and architectures. These elements are progressively tailored for specific mission areas, functionality, activities, and processes. Tailoring architectures promotes functional integration within and between the levels of the integration model. It helps ensure that users performing different functional activities work with systems that use a set of common architectures, standards, and services. Therefore, the users can use the planned global DoD network for meaningful information exchange and work together to achieve common objectives.

Figure 5-2 illustrates how the integration model can help achieve greater interoperability between functional activities in the DoD. The DoD is standardizing data and planning a global network at the Enterprise Level. The figure shows that different functional area applications will be able to access a common schema for shared databases maintained at the Enterprise Level and to use a global DoD network for information exchange. To the users of the functional activity applications, shared data will appear as part of the system they are using. Note, however, that each system may also have mission-area specific or unique data that may not be shared across functional lines.

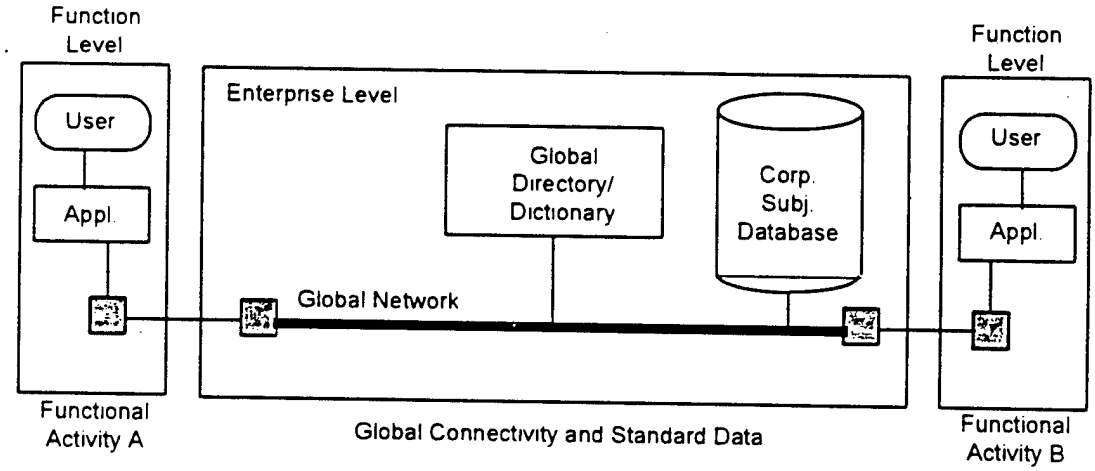


**Figure 5-2. Example of Functional and Technical Integration**

### 5.5.2 The Top-Down View

The top-down view of the integration model provides room for personal choice, innovation, and distributed development and control of systems by different organizations and individuals. The personal level can allow users to try out new ideas that may result in increased individual productivity. Procedures and technical controls will be used to control access to shared resources. The applications level develops, implements, and operates open systems using common methods, tools, and standards. Both shared and local applications can be developed. The function level provides the primary process models, data models, and information systems strategies for the DoD's functional activities. These elements are integrated into broader architectures that achieve cross-functional integration and interoperability. Each integration level inherits the characteristics of the upper integration levels.

## 5.6 ARCHITECTURE INTEGRATION AT LEVELS 1-3

Figure 5-3 shows the hierarchical structure of technical and other architectures, strategies, and plans that exist at each of the first three integration levels in the IM integration model. The architectures at lower levels guide and direct more specific architectures at the upper levels.

At Level 3, functional area activities can use a common architecture that is a subset of the functional area architecture. Functional areas can also use a common architecture that is a subset of the mission-area architecture.

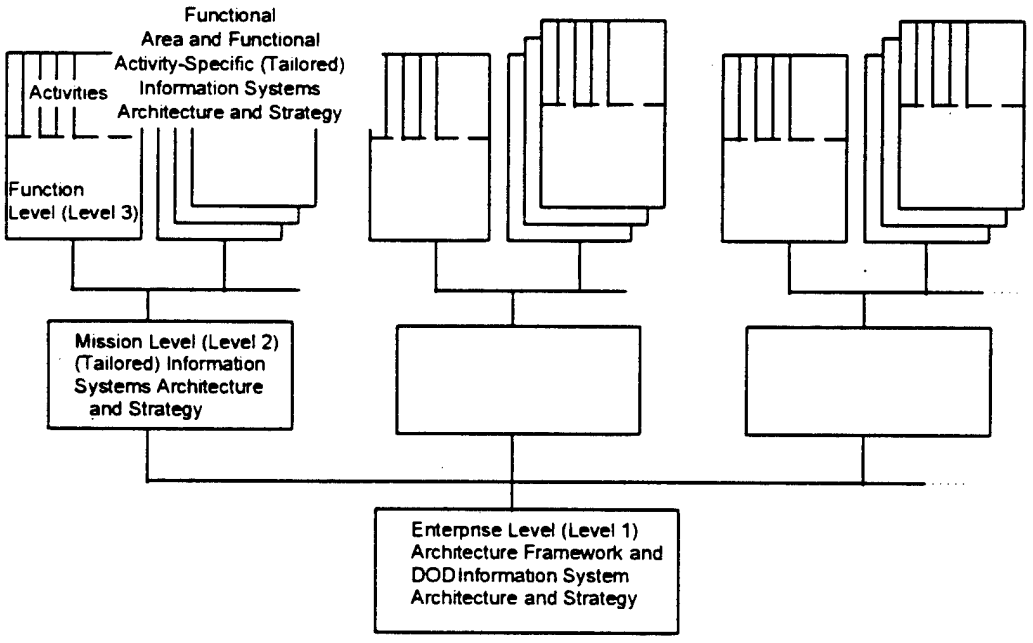


**Figure 5-3. Integration Levels of DoD IM Architectures and Strategies**

At Level 2, mission areas, such as C2, can use a common architecture that is a subset of the overall DoD architecture.

At Level 1, the DoD Enterprise Level, a common information system architecture can be established that results in increased interoperability, integration, sharing of resources, and overall warfighting and support effectiveness.

The integration process for achieving interoperability is guided by the IM integration model, which consists of the following generic steps:

- Architectures, strategies, and technical management planning information are developed for each Functional Activity under the direction and guidance of the FAPM.
- Functional activity and functional area architectures, strategies, and technical management planning information are reviewed by the DA and DISA for conformance with enterprise (DoD-wide) and mission-area architectures, strategies, and technical management planning information.
- Interoperability requirements of the individual systems are translated to mission critical criteria for testing purposes. Interoperability testing verifies that mission critical criteria are met.
- Approved data, application software, infrastructure, and information system architectures, strategies, and technical management planning information become part of the overall enterprise and mission-area architecture baseline. They are subject to IM technical integration and configuration management policies and procedures. They form a basis for interoperability and operational testing as a precursor to system certification for interoperability.
- Cross-functional information system integration strategies and plans are developed at the enterprise and mission levels under the guidance and direction of the DASD (IM). DoD mission areas, vision, strategies, and plans will be translated into technical architectures, strategies, and plans to provide guidance for the functional level.

An iterative process involving the participation of PSAs at the Enterprise Level, the JCS, DISA, and the DoD Components aligns and reconciles the enterprise, mission areas, and functional level planning, architecture, and control processes.

Over time, the computer and communications utility will grow in scope and capability to provide an ever-increasing percentage of all information services for the DoD. In the long-term, functional users will obtain information services at affordable costs because of few new development requirements. Furthermore, once integration has been fully refined and institutionalized in a common infrastructure for DoD, system development efforts will speed up, and time between system conceptualization and operation will be greatly reduced.

This page intentionally left blank.

# APPENDIX A

# REFERENCES

*Note: References appearing in this section represent documents used in preparation of the TAFIM, including some sources used at the time of initial document development that may no longer be current or applicable. The reader is advised to check the current applicability of a reference appearing in this list before using it as an information source. The reference section will be completely reviewed and revised for the next release of the TAFIM.*


1. Executive Level Group (ELG) for Defense Information Management, 30 September 1990, A Plan for Corporate Information Management for the Department of Defense.

2. Department of Defense Directive (DoDD) 4630.5, 12 November 1992, Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence (C3I) Systems.

3. DoDD 8000.1, 27 October 1992, Defense Information Management (IM) Program.

4. DoDD 8120.1, 14 January 1993, Life-Cycle Management (LCM) of Automated Information Systems (AISs).

5. DoDD 8320.1, 26 September 1991, DoD Data Administration.

6. DoD Instruction (DoDI) 4630.8, 18 November 1992, Procedures for Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence (C3I) Systems.

7. DoDI 8120.2, 14 January 1993, Automated Information System (AIS) Life-Cycle Management (LCM) Process, Review, and Milestone Approval Procedures.

8. DoD 8020.1-M (Draft), August 1992 with Change 1 of January 1993, Functional Process Improvement (Functional Management Process for Implementing the Information Management Program of the Department of Defense) and Interim Management Guidance on Functional Process Improvement.

9. DoD 7920.2-M, March 1990, Automated Information System Life-Cycle Management Manual.

10. DoD CIM Functional Economic Analysis (FEA) Guidebook, (Draft), 15 January 1993.

This page intentionally left blank.

# APPENDIX B

# GLOSSARY

The glossary consists of two parts: Acronyms and Definitions.

## ACRONYMS

| | |
|---|---|
| AIS | Automated Information System |
| AITS | Adopted Information Technology Standards |
| AMWG | Architecture Methodology Working Group |
| API | Application Program Interface |
| APP | Application Portability Profile |
| ASC | Accredited Standards Committee |
| ASD(C3I) | Assistant Secretary of Defense for Command, Control, Communications, and Intelligence |
| ASIS | Ada Semantic Interface Specification |
| BBS | Bulletin Board System |
| C2 | Command and Control |
| C3I | Command, Control, Communications, and Intelligence |
| CASE | Computer-Aided Software Engineering |
| CFA | Center for Architecture |
| CFII | Center for Integration & Interoperability |
| CIM | Corporate Information Management |
| CINC | Commander-in-Chief |
| CJCS | Chairman of the Joint Chiefs of Staff |
| CMP | Configuration Management Plan |
| COTS | Commercial-off-the-Shelf |
| DA | Data Administrator |
| DASD (IM) | Deputy Assistant Secretary of Defense for Information Management |
| DASP | Data Administration Strategic Plan |
| DDRS | Defense Data Repository System |
| DEPSECDEF | Deputy Secretary of Defense |
| DGSA | Department of Defense (DoD) Goal Security Architecture |
| DII | Defense Information Infrastructure |

| | |
|---|---|
| DISA | Defense Information Systems Agency |
| DISC | Defense Information System Council |
| DISN | Defense Information System Network |
| DISSP | Defense Information System Security Program |
| DoD | Department of Defense |
| DoDD | Department of Defense Directive |
| DoDI | Department of Defense Instruction |
| DODM | DoD Manual |
| | |
| E-mail | Electronic Mail |
| EDI | Electronic Data Interchange |
| EEI | External Environment Interface |
| ELG | Executive Level Guidance |
| | |
| FAPM | Functional Activity Program Manager |
| FEA | Functional Economic Analysis |
| FIPS | Federal Information Processing Standard |
| | |
| HCI | Human Computer Interface |
| | |
| I-CASE | Integrated Computer-Aided Software Engineering |
| IEEE | Institute of Electrical and Electronic Engineers |
| IM | Information Management |
| IS | Information System |
| ISA | Information System Architecture |
| ISO | International Organization for Standardization |
| IT | Information Technology |
| ITRUS | Information Technology Reuse |
| ITSI | Information Technology Standards Information |
| | |
| JCS | Joint Chiefs of Staff |
| JIEO | Joint Interoperability and Engineering Organization |
| JTC | Joint Technical Committee |
| JTC3A | Joint Tactical Command, Control and Communications Agency |
| | |
| LAN | Local Area Network |
| LCM | Life-Cycle Management |
| | |
| MOE | Measures of Effectiveness |
| MS | Microsoft |

| | |
|---|---|
| N | Notarization |
| NATO | North Atlantic Treaty Organization |
| OASD | Office for the Assistant Secretary of Defense |
| OSD | Office of the Secretary of Defense |
| OSE | Open Systems Environment |
| OSI | Open Systems Interconnection |
| PMP | Program Management Plan |
| PSA | Principal Staff Assistant |
| STD | Standard |
| T&E | Test and Evaluation |
| TA | Technical Architecture |
| TAFIM | Technical Architecture Framework for Information Management |
| TBD | To Be Determined |
| TCP/IP | Transmission Control Protocol/Internet Protocol |
| TCSEC | Trusted Computer System Evaluation Criteria |
| TDI | Trusted Database Interpretation |
| TFA | Transparent File Access |
| TLSP | Transport Layer Security Protocol |
| TMP | Technical Management Plan |
| TNI | Trusted Network Interpretation |
| TP | Traffic Padding |
| TRM | Technical Reference Model |
| TRI-TAC | Tri-Service Tactical Communications Systems |
| TSIG | Trusted Systems Interoperability Group |
| U.S. | United States |
| WWW | World Wide Web |

# DEFINITIONS

**Application**–The use of capabilities (services and facilities) provided by an information system specific to the satisfaction of a set of user requirements. [P1003.0/D15]

**Application Platform**–The collection of hardware and software components that provide the services used by support and mission-specific software applications.

**Application Portability Profile (APP)**–The structure that integrates Federal, national, international, and other specifications to provide the functionality necessary to accommodate the broad range of Federal information technology requirements. [APP]

**Application Program Interface (API)**–(1) The interface, or set of functions, between the application software and the application platform. [APP] (2) The means by which an application designer enters and retrieves information.

**Architecture**–Architecture has various meanings depending upon its contextual usage. (1) The structure of components, their interrelationships, and the principles and guidelines governing their design and evolution over time. [IEEE STD 610.12] (2) Organizational structure of a system or component. [IEEE STD 610.12]

**Architecture: Baseline and Target**–Defined and are significant parts of the technical management planning information (previously the technical management plan [TMP]). [DoD 8020.1-M with Change 1]

**Architecture, Database**–The logical view of the data models, data standards, and data structure. It includes a definition of the physical databases for the information system, their performance requirements, and their geographical distribution. [DoD 8020.1-M, Appendix J]

**Architecture Target**–Depicts the configuration of the target open information system. [DoD 8020.1-M]

**Architecture, Infrastructure**–Identifies the top-level design of communications, processing, and operating system software. It describes the performance characteristics needed to meet database and application requirements. It provides a geographic distribution of components to locations. The infrastructure architecture is defined by the service provider for these capabilities. It includes processors, operating systems, service software, and standards profiles that include network diagrams showing communication links with bandwidth, processor locations, and capacities to include hardware builds versus schedule and costs. [DoD 8020.1-M, Appendix J specifically paragraph 5(14)(c), Table J-2]

**Architectural Structure**–Provides the conceptual foundation of the basic architectural design concepts, the layers of the technical architecture, the services provided at each layer, the relationships between the layers, and the rules for how the layers are interconnected.

**Automated Information System (AIS)**–Computer hardware, computer software, telecommunications, information technology, personnel, and other resources that collect, record, process, store, communicate, retrieve, and display information. An AIS can include computer software only, computer hardware only, or a combination of the above. [DoDD 8000.1]

**Availability**–The probability that system functional capabilities are ready for use by a user at any time, where all time is considered, including operations, repair, administration, and logistic time. Availability is further defined by system category for both routine and priority operations. [JOPES ROC]

**Baseline**–A specification or product that has been formally reviewed and agreed upon, that thereafter serves as the basis for further development and that can be changed only through formal change control procedures or a type of procedure such as configuration management. [IEEE STD 610.12]

**Commercial-Off-the-Shelf (COTS)**–Refers to an item of hardware or software that has been produced by a contractor and is available for general purchase. Such items are at the unit level or higher. Such items must have been sold and delivered to government or commercial customers must have passed customer's acceptance testing, be operating under customer's control, and within the user environment. Further, such items must have meaningful reliability, maintainability, and logistics historical data.

**Communications Link**–The cables, wires, or paths that the electrical, optical, or radio wave signals traverse. [TA]

**Communications Network**–A set of products, concepts, and services, that enable the connection of computer systems for the purpose of transmitting data and other forms (e.g., voice and video) between the systems.

**Communications Node**–A node that is either internal to the communications network (e.g., routers, bridges, or repeaters) or located between the end device and the communications network to operate as a gateway. [TA]

**Communications Services**–A service of the Support Application entity of the Technical Reference Model (TRM) that provides the capability to compose, edit, send, receive, forward, and manage electronic and voice messages and real time information exchange services in support of interpersonal conferencing. [TA]

**Communications System**–A set of assets (transmission media, switching nodes, interfaces, and control devices), that will establish linkage between users and devices.

**Configuration Management**–A discipline applying technical and administrative direction and surveillance to: (a) identify and document the functional and physical characteristics of a configuration item, (b) control changes to those characteristics and, (c) record and report changes to processing and implementation status. [MIL-STD 973]

**Connectivity Service**–A service area of the External Environment entity of the Technical Reference Model that provides end-to-end connectivity for communications through three transport levels (global, regional, and local). It provides general and applications-specific services to platform end devices. [TA]

**Database Utility Service**–A Service of the Support Application Entity of the Technical Reference Model that provides the capability to retrieve, organize, and manipulate data extracted from a database. [TA]

**Data Dictionary**–A specialized type of database containing metadata, which is managed by a data dictionary system; a repository of information describing the characteristics of data used to design, monitor, document, protect, and control data in information systems and databases; an application of data dictionary systems. [DoDD 8320.1]

**Data Element**–A basic unit of information having a meaning and that may have subcategories (data items) of distinct units and values. [DoDD 8320.1]

**Data Interchange Service**–A service of the Platform entity of the Technical Reference Model that provides specialized support for the interchange of data between applications on the same or different platforms. [TA]

**Data Management Service**–A service of the Platform entity of the Technical Reference Model that provides support for the management, storage, access, and manipulation of data in a database. [TA]

**Directory Service**–A service of the External Environment entity of the Technical Reference Model that provides locator services that are restricted to finding the location of a service, location of data, or translation of a common name into a network specific address. It is analogous to telephone books and supports distributed directory implementations. [TA]

**Distributed Database**–(1) A database that is not stored in a central location but is dispersed over a network of interconnected computers. (2) A database under the overall control of a central database management system but whose storage devices are not all attached to the same processor. (3) A database that is physically located in two or more distinct locations. [FIPS PUB 11-3]

**Enterprise**–The highest level in an organization -- includes all missions and functions. [TA]

**Enterprise Model**–A high level model of an organization's mission, function, and information architecture. The model consists of a function model and a data model.

**External Environment Interface (EEI)**–The interface that supports information transfer between the application platform and the external environment. [APP]

**Function**–Appropriate or assigned duties, responsibilities, missions, tasks, powers, or duties of an individual, office, or organization. A functional area is generally the responsibility of a PSA (e.g., personnel) and can be composed of one or more functional activities (e.g., recruiting), each of which consists of one or more functional processes (e.g., interviews). [Joint Pub 1-02, DoDD 8000.1, and DoD 8020-1M]

**Functional Activity Program Manager (FAPM)**–FAPMs are designated by PSAs and are accountable for executing the functional management process. Supported by functional representatives from the DoD Components, FAPMs develop functional architectures and strategic plans, and establish the process, data, and information system baselines to support functional activities within the functional area. [DoD 8020.1-M Ch 1 B(2)]

**Functional Architecture**–The framework for developing applications and defining their interrelationships in support of an organization's information architecture. It identifies the major functions or processes an organization performs and their operational interrelationships. [DoD 5000.11-M]

**Functional Area**–A range of subject matter grouped under a single heading because of its similarity in use or genesis. [DoDD 8320.1]

**Functional Data Administrator (FDAd)**–Office of the Secretary of Defense (OSD) PSAs exercise or, designate functional data administrators to perform data administrator responsibilities to support execution of the functional management process, and to function within the scope of their overall assigned responsibilities. [DoDD 8320.1 and DoD 8020.1-M, Appendix A].

**Functional Economic Analysis (FEA)**–A structured proposal that serves as the principal part of a decision package for enterprise (individual, office, organization -see function) leadership. It includes an analysis of functional process needs or problems; proposed solutions, assumptions, and constraints; alternatives; life-cycle costs; benefits and/or cost analysis; and investment risk analysis. It is consistent with, and amplifies, existing DoD economic analysis policy. [DoDI 7041.3, DoDD 8000.1, and DoD 8020.1-M, Appendix H]

**Hardware**–(1) Physical equipment, as opposed to programs, procedures, rules, and associated documentation. (2) Contrast with software [FIPS PUB 11-3]

**Information**–Any communication or representation of knowledge such as facts, data; or opinions, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms. [OMB CIRC A-130]

**Information Domain**–A set of commonly and unambiguously labeled information objects with a common security policy that defines the protections to be afforded the objects by authorized users and information management systems. [DISSP]

**Information Management** (IM)–The creation, use, sharing, and disposition of information as a resource critical to the effective and efficient operation of functional activities. The structuring of functional processes to produce and control the use of data and information within functional activities, information systems, and computing and communications infrastructures. [DoDD 8000.1]

**Information Resources Management (IRM)**–The planning, budgeting, organizing, directing, training, promoting, controlling, and management activities associated with the burden (cost), collection, creation, use, and dissemination of information by Agencies and includes the management of information and related resources, such as Federal information processing (FIP) resources. [PL No 99-591, DoDD 8000.1.]

**Information Technology (IT)**–The technology included in hardware and software used for Government information, regardless of the technology involved, whether computers, communications, micro graphics, or others. [OMB Circular A-130 and DoDD 8000.1.]

**Infrastructure**–Infrastructure is used with different contextual meanings. Infrastructure most generally relates to and has a hardware orientation but note that it is frequently more comprehensive and includes software and communications. Collectively, the structure must meet the performance requirements of and capacity for data and application requirements. Again note that just citing standards for designing an architecture or infrastructure does not include functional and mission area requirements for performance. Performance requirement metrics must be an inherent part of an overall infrastructure to provide performance interoperability and compatibility. It identifies the top-level design of communications, processing, and operating system software. It describes the performance characteristics needed to meet database and application requirements. It provides a geographic distribution of components to locations. The infrastructure architecture is defined by the service provider for these capabilities. It includes processors, operating systems, service software, and standards profiles that include network diagrams showing communication links with bandwidth, processor locations, and capacities to include hardware builds versus schedule and costs. [DoD 8020.1-M]

**Integration**–Integration is the result of an effort that joins two or more similar products such as individual system elements, components, modules, processes, databases, or other entities, and produces a new product that functions, as a replacement for the two or more similar but less capable entities (products), in a framework or architecture in a seamless manner. Institute of Electrical and Electronic Engineers (IEEE) Standard (STD) 610.12 defines an "integration architecture" as a framework for combining software components, hardware components, or both into an overall system. [IEEE STD 610.12]

**Interoperability**–(1) The ability of two or more systems or components to exchange and use information. [IEEE STD 610.12]. (2) The ability of the systems, units, or forces to provide and receive services from other systems, units, or forces, and to use the services so interchanged to enable them to operate effectively together. The conditions achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users. [Joint Pub 1-02, DoD/NATO] [JOPES ROC]

**Legacy Environments**–Legacy environments could be called legacy architectures or infrastructures and as a minimum consist of a hardware platform and an operating system. Legacy environments are identified for phase-out, upgrade, or replacement. All data and applications software that operate in a legacy environment must be categorized for phase-out, upgrade, or replacement.

**Legacy Systems**–Systems that are candidates for phase-out, upgrade, or replacement. Generally legacy systems are in this category because they do not comply with data standards or other standards. Legacy system workloads must be converted, transitioned, or phased out (eliminated). Such systems may or may not operate in a legacy environment.

**Life Cycle**–The period of time that begins when a system is conceived and ends when the system is no longer available for use. [IEEE STD 610.12] AIS life cycle is defined within the context of life-cycle management in various DoD publications. It generally refers to the usable system life.

**Local Area Network (LAN)**–A data network, located on a user's premises, within a limited geographic region. Communication within a local area network is not subject to external regulation; however, communication across the network boundary may be subject to some form of regulation. [FIPS PUB 11-3]

**Migration Systems**–An existing AIS, or a planned and approved AIS, that has been officially designated to support common processes for a functional activity applicable to use DoD-wide or DoD Component-wide. Systems in this category, even though fully deployed and operational, have been determined to accommodate a continuing and foreseeable future requirement and, consequently, have been identified for transitioning to a new environment or infrastructure. A migration system may need to undergo transition to the standard technical environment and standard data definitions being established through the Defense IM Program, and must "migrate" toward that standard. In that process it must become compliant with the Reference Model and the Standards Profile. A system in this category may require detailed analysis that involves a total redesign, reprogramming, testing, and implementation because of a new environment and how the "users" have changed their work methods and processes. The detailed analysis may identify the difference between the "as is" and the "to be" system. [DoD 8020.1-M.]

**Multimedia Service**–A service of the TRM that provides the capability to manipulate and manage information products consisting of text, graphics, images, video, and audio. [TA]

**Open Specifications**–Public specifications that are maintained by an open, public consensus process to accommodate new technologies over time and that are consistent with international standards. [P1003.0/D15]

**Open System**–A system that implements sufficient open specifications for interfaces, services, and supporting formats to enable properly engineered applications software: (a) to be ported with minimal changes across a wide range of systems, (b) to interoperate with other applications on local and remote systems, and (c) to interact with users in a style that facilitates user portability. [P1003.0/D15]

**Open Systems Environment (OSE)**–The comprehensive set of interfaces, services, and supporting formats, plus user aspects for interoperability or for portability of applications, data, or people, as specified by information technology standards and profiles. [P1003.0/D15]

**Operating System Service**–A core service of the Platform entity of the Technical Reference Model that is needed to operate and administer the application platform and provide an interface between the application software and the platform (e.g., file management, input/output, print spoolers). [TA]

**Platform**–The entity of the Technical Reference Model that provides common processing and communication services that are provided by a combination of hardware and software and are required by users, mission area applications, and support applications. [TA]

**Portability**–(1) The ease with which a system or component can be transferred from one hardware or software environment to another. [IEEE STD 610.12] (2) A quality metric that can be used to measure the relative effort to transport the software for use in another environment or to convert software for use in another operating environment, hardware configuration, or software system environment. [IEEE TUTOR] (3) The ease with which a system, component, data, or user can be transferred from one hardware or software environment to another. [TA]

**Process Model**–Provides a framework for identifying, defining, and organizing the functional strategies, functional rules, and processes needed to manage and support the way an organization does or wants to do business -- provides a graphical and textual framework for organizing the data and processes into manageable groups to facilitate their shared use and control throughout the organization. [DoD 5000.11-M]

**Profile**–A set of one or more base standards, and, where applicable, the identification of those classes, subsets, options, and parameters of those base standards, necessary for accomplishing a particular function. [P1003.0/D15]

**Profiling**–Selecting standards for a particular application. [P1003.0/D15]

**Response Time**–The ability to react to requests within established time criteria. To be operationally effective, the system must product the desired output in a timely manner based on system category for routine or priority operations. [JOPES ROC]

**Scalability**–The ability to use the same application software on many different classes of hardware/software platforms from personal computers to super computers (extends the portability concept). [USAICII] The capability to grow to accommodate increased work loads.

**Seamless Interface**–Ability of facilities to call one another or exchange data with one another in a direct manner. Integration of the user interface that allows a user to access one facility through another without any noticeable change in user interface conventions. [DSAC SYS IM]

**Stovepipe System**–A system, often dedicated or proprietary, that operates independently of other systems. The stovepipe system often has unique, nonstandard characteristics.

**System**–People, machines, and methods organized to accomplish a set of specific functions. [FIPS PUB 11-3]

**System Management Service**–A service of the Platform entity of the TRM that provides for the administration of the overall information system. These services include the management of information, processors, networks, configurations, accounting, and performance. [TA]

**Technical Reference Model (TRM)**–The document that identifies a target framework and profile of standards for the DoD computing and communications infrastructure. [TRM]

**User**–(1) Any person, organization, or functional unit that uses the services of an information processing system. (2) In a conceptual schema language, any person or any thing that may issue or receive commands and messages to or from the information system. [FIPS PUB 11-3]

**User Interface Service**–A service of the Platform entity of the Technical Reference Model that supports direct human-machine interaction by controlling the environment in which users interact with applications. [TA]

This page intentionally left blank.

# APPENDIX C

# VISION FOR DOD INFORMATION MANAGEMENT

Section 3.0 focused on the vision for information technology. This appendix focuses on the vision for information management. A significant aspect of Section 3.0 addresses the management of information technology. Overall, the visions include the use of information technology to manage information. For example, information technology enables functional managers to standardize and streamline processes and activities, reduce non-value-added work, improve productivity, and lower costs for operations across the DoD. Information management is critical to providing efficient and effective information functional processes and practices across the DoD. It is recognized as a force effectiveness and support multiplier during peacetime preparedness, transition to war, and war. The integration of information management principles with technologies into all aspects of DoD operations means that effective military capability is maintained while defense budgets decline.

Functional methods and measures are being updated and documented across the DoD. Options and opportunities to standardize, simplify, and improve processes and management practices will be identified and selected at all levels using process modeling, process improvement, and functional economic analysis methods.

Measures of performance will be used to manage functions and systems resulting in improved quality, productivity, cost performance, and functionality. The mechanisms to capture performance data are built into information systems, enabling managers to evaluate their effectiveness and make continuous improvements. Comprehensive evaluations will be performed continuously throughout the system life cycle to ensure the systems continue to meet the functional needs of the users

Data standards are being established and implemented across the mission areas. A data modeling initiative will result in providing standard data descriptions and attributes captured in a DoD-wide Defense Data Repository System (DDRS). With common data definitions, data reuse will become the standard practice in all systems development and maintenance. All forms of data, including alphanumeric, geographic, document format, and multi-media are managed for interoperability and meaningful exchange within and across functions. Standard data definitions and models are being developed with industry and other parts of the Federal Government.

DoD will implement shared corporate databases that capture, store, and maintain standard data. Data will be input at the source for accuracy and validity and reused whenever possible. Horizontal and perpendicular data transformations will be controlled and included in the data repository. Data will be input through a variety of flexible and responsive devices and mechanisms from the office to the battlefield. Electronic capture and display of information, which is becoming normal practice, will lead to a "less-paper" (and in some cases a "paper-less")

DoD environment. Currency, reliability, and responsiveness are being greatly improved, errors avoided, and the integrity and security of DoD data will be assured by new procedures and automation.

Users will eventually access data through a common global network, and through other media such as CD-ROM, limited only by their need to know. The physical location of data will become transparent to users and applications. A DoD directory and dictionary capability maintains global and functional schemas for the corporate database. A total information management facility will be established to filter, process, distribute, and fuse information when and where it is needed.

Electronic data interchange (EDI) of all forms of information is planned and will be implemented following the world-wide lead of industry. Transaction systems that automatically process specific tasks will be common. These capabilities will reduce manual work, eliminate errors, and improve the performance of complex operational activities. For example, DoD will routinely conduct most of its business with industry suppliers through electronic commerce and technical document interchange. Artificial intelligence will become critical to many functions, enabling processes to be substantially automated.

The foundation of standard processes and data, and new technologies, will enable a variety of typical functions to be performed far more effectively and efficiently. For example,

- Office automation will benefit from a suite of standards-based, flexible and integrated word processing, graphics, document preparation, and groupware applications.

- Decision support to managers and commanders will provide benefits from video-conferencing (to the desktop when necessary), mail services, briefing preparation and display facilities, and modeling and simulation capabilities.

- The operational commander will benefit from the DoD-wide technical capabilities to pull, fuse, filter, and disseminate the precise information needed to address situation-dependent missions.

- A rapid, responsive, efficient, and quality-oriented AIS life-cycle development and maintenance process is being instituted. This process is based on certain key practices such as:

  - Process modeling and functional economic analysis

  - Data administration procedures, practices, and standard data elements in a DoD DDRS

  - Open systems environments, architectures and implementations

  - Integrated computer-aided software engineering (CASE) methods and tools

- Streamlined software processes, metrics, and reuse
- Streamlined information technology reuse and acquisition
- Shared design, processing, network, and information center
- Services (i.e., a utility) delivered on a fee-for-service basis.

The roles and responsibilities of functional and technical managers, developers, and operators have been structured to leverage the strengths of each. Technical integration management support to functional activity managers is key to helping them plan integrated information systems support within and across functions. Information technologists provide the required tools and building blocks needed to develop, install, and operate efficient and effective information systems.

This page intentionally left blank.

# APPENDIX D

## DOD MEMORANDA ADDRESSING USE OF THE TAFIM

This appendix contains the text of three DoD memoranda that address the use of the TAFIM:

- 30 March 1995 Memorandum from the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence
- 12 November 1993 Memorandum from the Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (with attachment)
- 13 October 1993 Memorandum from the Deputy Secretary of Defense (with attachment).

This page intentionally left blank.

# MEMORANDUM FROM
# THE ASSISTANT SECRETARY OF DEFENSE

March 30, 1995

MEMORANDUM FOR
UNDER SECRETARIES OF DEFENSE
ASSISTANT SECRETARY OF THE ARMY (RD&A)
ASSISTANT SECRETARY OF THE NAVY (RD&A)
ASSISTANT SECRETARY OF THE AIR FORCE
(ACQUISITION ) (SAF/AQ)
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTOR, JOINT STAFF

SUBJECT: Technical Architecture Framework for Information Management (TAFIM), Version 2.0

My memorandum dated June 23, 1994 established the TAFIM as the single framework to promote the integration of Department of Defense (DoD) information systems, expanding the opportunities for interoperability and enhancing our capability to manage information resources across the Department. The latest version of the TAFIM, Version 2.0, is complete and fully coordinated. Version 2.0 consists of seven volumes as shown in the attachment. The TAFIM will continue to guide and enhance the evolution of the Department's information systems technical architectures.

I want to reiterate two important points that I made in my June 1994 memorandum. First, the Department remains committed to a long range goal of an open systems environment where interoperability and cross functional integration of our systems and portability/reusability of our software are key benefits. Second, the further selection and evaluation of migration systems should take into account this long range goal by striving for conformance to the TAFIM to the extent possible.

Effectively immediately, new DoD information systems development and modernization programs will conform to the TAFIM. Evolutionary changes to migration systems will be governed by conformance to the TAFIM.

The TAFIM is maintained by the Defense Information Systems Agency (DISA) and is available electronically via the DISA On-Line Standards Library. Hardcopy is available through the Defense Technical Information Center. The TAFIM is an evolving set of documents and comments for improving may be provided to DISA at any time. The DISA action officer is Mr. Bobby Zoll, (703) 735-3552. The OSD action officer is Mr. Terry Hagle, (703) 604-1486.

s/Emmett Paige, Jr.

# MEMORANDUM FROM
# THE ASSISTANT SECRETARY OF DEFENSE

November 12, 1993

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DIRECTOR, DEFENSE RESEARCH AND ENGINEERING
ASSISTANT SECRETARIES OF DEFENSE
COMPTROLLER
GENERAL COUNSEL
INSPECTOR GENERAL
DIRECTOR, OPERATIONAL TEST AND EVALUATION
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR OF ADMINISTRATION AND MANAGEMENT
DIRECTORS OF THE DEFENSE AGENCIES

SUBJECT: Selection of Migration Systems

This memorandum provides the generic evaluation criteria to be used in selection of migration systems as required by the Deputy Secretary of Defense (DEPSECDEF) memorandum of 13 October 1993, "Accelerated Implementation of Migration Systems, Data Standards, and Process Improvement." The Department of Defense (DoD) must improve the quality and effectiveness of information support for our fighting forces, reduce the cost of duplicative processes, eliminate nonessential legacy systems in all functional areas, and minimize the cost and difficulty of information systems technical integration. Information systems are comprised of applications, data and infrastructure. Expedited selection of migration systems has been established by the Deputy Secretary of Defense as a matter of urgency throughout the DoD. Selection shall be based on these four factors:

- Functional: To be selected as a migration system, the information system will have to be based on defined work processes and will have to be based on the degree to which the system meets the information needs of users within and across functional areas. A decision should be generally supported by the functional user community within the DoD Components, including the Chairman of the Joint Chiefs of Staff (CJCS) representing the unified combatant commands.

- Technical: The system can evolve (migrate) to be supported by the integrated, standards-based architecture prescribed for the future Defense Information Infrastructure (DII).

- Programmatic: A functional economic analysis that documents a reasonable range of alternatives that meet both functional and technical objectives is required. The alternatives

must be within programmatic constraints (resources, schedules, and acquisition strategy), and justify adopting the migration system to the Department. Given the compressed time frames, the PSAs may elect to base their migration decision on an abbreviated functional economic analysis. Acquisition strategy planning factors will be considered in accordance with Acting ASD($C^3$I) memorandum of February 4, 1993, "Acquisition Strategy Planning for CIM Migration Systems."

- Data: The ability to transition to data standards is a fundamental requirement for an information system in order for it to be selected as a migration system. Applications should lend themselves to data sharing within their design. Migration plans must include transition to DoD standard data and shared data concepts.

Migration systems selection procedures and factors are discussed in our Interim Management Guidance on Functional Process Improvement (August 5, 1992, and January 15, 1993). Except where exempted under DoD Directive 8120.1, Section B, the selection procedures apply to all AISs in the Department. This includes all $C^3$I systems except those specifically and individually exempted by me in accordance with my DoD Senior Information Management (IM) authority under DoD Directives 5137.1 and 8000.1. All information technology services shall be transition to the selected migration systems over a period not to exceed three years, and the legacy systems providing these services shall be terminated. Any funding for development, modernization, or enhancement of these legacy systems requires the approval of the DoD Senior IM Official, in accordance with the DEPSECDEF's memorandum of October 13, 1993. Life-cycle management reviews of migration systems shall also address these candidate legacy systems and data until their termination.

Migration system selection shall be made by the Office of the Secretary of Defense (OSD) Principal Staff Assistant(s) (PSAs), or CJCS, having functional responsibility for the missions and functions supported by the system, with the participation of affected DoD Components. The choice of functional criteria guidance in the selection of migration systems is the responsibility of the PSAs/CJCS. As the DoD Senior IM Official, I shall approve the proposed selection, based on my review of the selecting official's evaluation of technical, programmatic, and data factors. Because technical factors are critical to successful implementation of the DII, I shall have additional studies conducted where appropriate, and I shall withhold my approval where significant issues remain unresolved. Disagreements shall be resolved in accordance with DoD Directive 8000.1, Section E.1.d.

Attached to this memorandum are key technical considerations that must be addressed in the selection process. Assistance in your selection of migration systems and in preparation of the appropriate documentation is available through the Defense Information Systems Agency Center for Integration and Interoperability. If you would like this assistance, please contact Dr. Michael Mestrovich at (703) 756-4740.

s/Emmett Paige, Jr.

Attachment

# KEY TECHNICAL FACTORS TO BE CONSIDERED IN THE SELECTION OF MIGRATION SYSTEMS

## Technical Factors

Extent to which the candidate legacy automated information system (including Command, Control, Communications and Intelligence ($C^3I$) systems) currently conforms to, or can evolve (migrate) to conformance with, the open systems environment and standards-based architecture defined by the DoD Technical Architecture Framework for Information Management (TAFIM)[1].

Difficulty, cost, and time line for migrating the system (including its applications, data, and supporting infrastructure) as expeditiously as possible from its current technical environment to conformance with:

- The TAFIM.
- DoD standard data, based on the DoD Data Model. The DoD Data Model is a principal component of the DoD Enterprise Model.
- Shared use of applications, databases, and the computing and communications infrastructure with other designated migration systems.
- Cost effective, timely, secure, and highly reliable support to all functional users from consolidated data processing facilities.

Timeliness, completeness, and availability of life-cycle management and supporting documentation, particularly including data and application software documentation.

Difficulty, cost, and time line for application of:

- DoD information technology utility services.
- Commercial-off-the-shelf (COTS) software, and portable, re-usable software modules.
- Ada and computer-aided software engineering (CASE) tools and methods.

Current and future interface, interoperability, and integration requirements with other systems and databases within and across all DoD functional activities and functional areas.

---

[1] Office of the Assistant Secretary of Defense ($C^3I$) Memorandum, "Interim Management Guidance on the Technical Architecture Framework for Information Management (TAFIM)," January 15, 1993.

### Application of Technical Factors

Application of these technical factors results in giving preference to systems that:

- Have been developed using Ada and other "state of the industry" software engineering best practices, are well documented, and are under good configuration control.
- Use current COTS information technology software and hardware, such as data dictionaries and data base management systems, optical disk technology, etc.
- On the whole, are more compliant rather than less compliant with the technical factors listed above, and apply those factors consistently across all systems supporting the functional area.

### Assessment and Plans

The selection of a candidate migration AIS must be founded on its functional and technical adequacy. Migration assessment includes a technical analysis of migration candidate systems to ensure legacy applications will meet the information requirements of the functional user and that has the ability to accommodate subsequent functional and technical improvement activities.

A migration plan consisting of functional, technical and data concerns, with programmatic considerations is the start of the process for selecting migration systems. The DoD "Tree" diagrams, a quarterly publication from DISA/Center for Integration and Interoperability (CFII), displays each functional area's decisions for integrating. These "Tree" diagrams will be completed by all functional areas with target dates to depict the Enterprise Integration. The diagrams present an important migration picture but stop short of the migration planning that is necessary for implementation. The DISA/CFII is available to help each functional area develop migration plans and assess technical cross-functional integration for the Enterprise.

To validate the technical sufficiency of a candidate migration system, the applications should be evaluated in terms of relevant functional, technical, data handling, and programmatic criteria.

# ATTACHMENTMEMORANDUM FROM THE DEPUTY SECRETARY OF DEFENSE

13 October 1993

MEMORANDUM FOR
SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
ASSISTANT TO SECRETARIES OF DEFENSE
COMPTROLLER
GENERAL COUNSEL
INSPECTOR GENERAL
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR OF ADMINISTRATION AND MANAGEMENT
DIRECTORS OF THE DEFENSE AGENCIES

SUBJECT: Accelerated Implementation of Migration Systems, Data Standards, and Process Improvement

My May 7, 1993, memorandum reiterated the full commitment of the Department of Defense (DoD) to the "... improvements, efficiencies, and productivity that are the essence of CIM." The focus of Corporate Information Management (CIM) on functional process improvement, migration systems, and data standardization has my full support. We need to get on with the job. In order to offset our declining resources, we must accelerate the pace at which we define standard baseline process and data requirements, select and deploy migration systems, implement data standardization, and conduct functional process improvement reviews and assessments (business process re-engineering) within and across all functions of the Department. The acceleration of these actions is key to containing the functional costs of performing the DoD mission within our constrained budget.

The attached guidance requires that addressees expedite selection of standard migration systems and standard data as the basis for process improvement reviews and assessments. The attached guidance expands on direction previously issued by the Comptroller on June 25, 1990, and by the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) (ASD($C^3$I)) on February 11, 1991. The ASD($C^3$I) will work with you to ensure that overall functional and Component requirements are met and balanced as we integrate and improve systems, data, and processes across the DoD. Our near-term strategy requires:

- Selection of migration systems within six months, with follow-on DoD-wide transition to the selected systems over a period not to exceed three years.
- Complete data standardization within three years by simplifying data standardization procedures, reverse engineering data requirements in approved and proposed migration

systems, and adopting standard data previously established by individual functions and Components for DoD-wide use wherever practical.

The above actions should be implemented immediately, and given appropriate priority in your current and future resource planning and allocation.

Ongoing information management initiatives such as functional process improvement projects, functional and technical integration analysis and planning, and software engineering methods modernization should continue on an expedited basis. However, completion of these current initiatives will not be prerequisites to implementation of the migration system and data standards acceleration strategy. Once standard DoD-wide process, system, and data baselines are established, process improvement studies will be more productive and study results can be more rapidly implemented.

It is understood that the implementation of standard migration systems may result in the loss of automated functionality by selected system users, whereas others may gain functionality. Loss of functionality should not be used as a reason to delay migration system selection and deployment unless there is a documented adverse impact on readiness within the deployment period, or an inability to comply with the law.

The ASD($C^3I$) is responsible for supplementing existing procedures with generic evaluation criteria within 30 days to be used in selecting migration systems, and ensuring the objectivity of the selection process.

I request that you personally ensure these actions are accomplished on schedule, and that you report to me on your progress by January 31, 1994.

s/William J. Perry

Attachment

# DEPARTMENT OF DEFENSE

# STRATEGY FOR ACCELERATION OF MIGRATION SYSTEMS AND DATA STANDARDS

## OBJECTIVE

Improve the quality and utility of DoD information while reducing the annual cost of DoD operations.

## STRATEGY

### Migration Systems

- OSD Principal Staff Assistants, together with their Defense Component counterparts, will, by March 31, 1994, select an information system(s) for each of their respective functional areas of responsibility for designation as the standard, DoD-wide migration system.

- Concurrently, OSD Principal Staff Assistants will develop plans to transition all information technology services throughout the DoD to the selected migration systems, over a period not to exceed three years. Draft plans will be circulated to other Principal Staff Assistants and to Defense Components so that cross-functional and other implementation issues can be identified for consideration by functional and Defense Component members of the DoD corporate Functional Integration Board, chaired by the Deputy Assistant Secretary of Defense (Information Management).

- Funding for development, modernization, or enhancement of legacy systems not selected to be migration systems will be stopped except where approved by the DoD Senior Information Management Official as absolutely essential to support DoD missions or comply with the law.

- The plan for implementing and transitioning services to the selected migration systems should simultaneously forecast a schedule, to the extent practical, for incorporating within the migration systems:

  - Improved functionality and cross-functional integration based on accelerated process improvement reviews and assessments.

  - Interoperability, technical integration, DoD standard data, and integrated databases to provide higher quality and lower cost information technology services for all users.

- Where a requirement is demonstrated to develop a follow-on, new start system to replace the standard migration system in order to meet CIM objectives and the information management policies and principles established in DoD Directive 8000.1, OSD Principal

Staff Assistants will conduct the necessary process improvement studies to develop functional requirements within the next three years.

**Data Standardization**

- Each DoD Principal Staff Assistant, together with their Defense Component counterparts, will develop and execute a plan in accordance with DoD Directive 8320.1 to standardize the data elements for which they are the custodian within the next three years.

- The ASD($C^3I$) will, by January 31, 1994, develop simplified and streamlined processes for data standardization and data administration within the DoD.

- In the interim, the Department will continue to use the existing standard data elements within each function and Defense Component that have been developed under previous procedures. These interim standard data elements are the data standards until replaced by those prepared under DoD Directive 8320.1.

## DEFINITIONS

The definitions below are intended to clarify the terms used in the DoD near-term strategy for acceleration of migration systems and data standards. Formal definitions are published in DoD directives or other publications.

**Baseline Processes and Data**

A baseline is something that has been formally reviewed and agreed upon, that thereafter serves as the basis for further development, and that can be changed only through formal change control procedures. Baseline processes and data establish how a function operates today (the "as is" environment), and what current functional requirements must be satisfied by the supporting migration system. Process improvement projects assess the "as is" baseline to determine what improvements should be made (to the "to be" environment). Once these improvements have been implemented, they define a new process and data baseline for the next iteration of improvements.

**Data Standard** (also called standard data)

A data element that has been through a formal analysis (called "data standardization") to reach agreement on its name, meaning, and characteristics, as well as its relationship to other standard data elements. Much like a common language, data standards enable processes and their supporting information systems to be integrated across functions, as well as within them, and improve the quality as well as the productivity of enterprise performance.

**Data Standardization**

The process of reviewing and documenting the names, meanings, and characteristics of data elements so that all users of the data have a common, shared understanding of it.

Data standardization is a critical part of the DoD Data Administration Program, managed under DoD Directive 8320.1. Data administration is the function that manages the definition and organization of the Department's data.

**Function**

Appropriate or assigned duties, responsibilities, and tasks that produce products or provide services. In the DoD, a functional area (e.g., personnel) is comprised of one or more functional activities (e.g., recruiting), each of which consists of one or more functional processes (e.g., interviewing candidates). The functions of the DoD are the responsibility of designated officials who exercise authority over organizations set up to accomplish their assigned functions. The structure and interrelationships among DoD functions and standard data are documented in the DoD Enterprise Model.

Individual functions within the DoD rely on other functions for products and services. In a large, complex enterprise such as the Department of Defense, functions must work together to support the mission of the enterprise; this significantly increases the importance of cross-functional programs, such as data standardization.

**Functional Process Improvement** (also called business process re-engineering)

Application of a structured methodology to define a function's objectives and a strategy for achieving those objectives; its "as is" and "to be" process and data environments; its current and future mission needs and end user requirements; and a program of incremental and evolutionary improvements to processes, data, and supporting migration systems that are implemented through functional, technical, and economic analysis and decision-making.

Procedures for conducting process improvement reviews and assessments in the DoD are provided in OASD($C^3I$) memoranda on Interim Management Guidance on Functional Process Improvement (August 5, 1992, and January 15, 1993).

**Integration**

Explicit top management initiatives to ensure that interdependent functions or systems operate effectively and efficiently for the overall benefit of the enterprise (i.e., the DoD). This contrasts with coordination among functions or systems, which ensures non-interference, but does not provide integration.

"Integration" implies seamless, transparent operation based on a shared or commonly-derived architecture (functional or technical) and standard data. "Interoperability" implies only the ability of a function or system to exchange information or services with another, separate function or system using translators or interchange rules/standards.

## Migration System

An existing automated information system (AIS), or a planned and approved AIS, that has been officially designated as the single AIS to support standard processes for a function. Other AISs, called "legacy systems," that duplicate the support services provided by the migration system are terminated, so that all future AIS development and modernization can be applied to the migration system. A migration system is designated (or selected) by the OSD Principal Staff Assistant(s) and their Defense Component counterparts whose function(s) the system supports, with the coordination of the DoD Senior Information Management Official.

Upon selection and deployment, the migration system becomes the single AIS baseline for:

- Incremental and evolutionary changes that are required to implement functional process improvements, or to execute additional responsibilities assigned to the function that the system supports.

- Technical enhancements that implement standard data and integrated databases, and that migrate the system toward an open systems environment and a standards-based architecture defined by the DoD Technical Architecture Framework for Information Management.

Requirements for selection of migration systems are identified in Chapters 6 and 7 of OASD($C^3I$) memoranda on Interim Management Guidance for Functional Process Improvement (August 5, 1992, and January 15, 1993); these procedures should be tailored as appropriate to facilitate expeditious selection. Subsequent development and modernization of migration systems is accomplished in accordance with DoD Directive 8120.1 and DoD Instruction 8120.2.

This page intentionally left blank

# APPENDIX E

# PROPOSING CHANGES TO TAFIM VOLUMES

## E.1 INTRODUCTION

Changes to the TAFIM will occur through changes to the TAFIM documents (i.e., the TAFIM numbered volumes, the Configuration Management Plan (CMP), and the Program Management Plan (PMP)). This appendix provides guidance for submission of proposed TAFIM changes. These proposals should be described as specific wording for line-in/line-out changes to a specific part of a TAFIM document.

Use of a standard format for submitting a change proposal will expedite the processing of changes. The format for submitting change proposals is shown in Section E.2. Guidance on the use of the format is provided in Section E.3.

A Configuration Management contractor is managing the receipt and processing of TAFIM change proposals. The preferred method of proposal receipt is via electronic mail (E-mail) in American Standards Code for Information Interchange (ASCII) format, sent via the Internet. If not e-mailed, the proposed change, also in the format shown in Section E.2, and on both paper and floppy disk, should be mailed. As a final option, change proposals may be sent via fax; however, delivery methods that enable electronic capture of change proposals are preferred. Address information for the Configuration Management contractor is shown below.

Internet: **tafim@bah.com**

Mail: **TAFIM**
**Booz•Allen & Hamilton Inc.**
**5201 Leesburg Pike, 4th Floor**
**Falls Church, VA 22041**

Fax: **703/824-3770**, indicate "TAFIM" on cover sheet.

## E.2 TAFIM CHANGE PROPOSAL SUBMISSION FORMAT

**a. Point of Contact Identification**

(1) Name:

(2) Organization and Office Symbol:

(3) Street:

(4) City:

(5) State:

(6) Zip Code:

(7) Area Code and Telephone #:

(8) Area Code and Fax #:

(9) E-mail Address:

**b. Document Identification**

(1) Volume Number :

(2) Document Title:

(3) Version Number:

(4) Version Date:

**c. Proposed Change # 1**

(1) Section Number:

(2) Page Number:

(3) Title of Proposed Change:

(4) Wording of Proposed Change:

(5) Rationale for Proposed Change:

(6) Other Comments:

**d. Proposed Change # 2**

(1) Section Number:

(2) Page Number:

(3) Title of Proposed Change:

(4) Wording of Proposed Change:

(5) Rationale for Proposed Change:

(6) Other Comments:

**n. Proposed Change # n**

(1) Section Number:

(2) Page Number:

(3) Title of Proposed Change:

(4) Wording of Proposed Change:

(5) Rationale for Proposed Change:

(6) Other Comments:

## E.3 FORMAT GUIDANCE

The format in Section E.2 should be followed exactly as shown. For example, Page Number should not be entered on the same line as the Section Number. The format can accommodate, for a specific TAFIM document, multiple change proposals for which the same individual is the Point of Contact (POC). This POC would be the individual the TAFIM project staff could contact on any question regarding the proposed change. The information in the **Point of**

**Contact Identification** part (**E.2 a)** of the format would identify that individual. The information in the **Document Identification** part of the format (**E.2 b**) is self-evident, except that volume number would not apply to the CMP or PMP. The proposed changes would be described in the **Proposed Change #** parts (**E.2 c, E.2 d, or E.2 n**) of the format.

In the **Proposed Change #** parts of the format, the Section number refers to the specific subsection of the document in which the change is to take place (e.g., Section 2.2.3.1). The page number (or numbers, if more than one page is involved) will further identify where in the document the proposed change is to be made. The Title of Proposed Change field is for the submitter to insert a brief title that gives a general indication of the nature of the proposed change. In the Wording of Proposed Change field the submitter will identify the specific words (or sentences) to be deleted and the exact words (or sentences) to be inserted. In this field providing identification of the referenced paragraph, as well as the affected sentence(s) in that paragraph, would be helpful. An example of input for this field would be: "Delete the last sentence of the second paragraph of the section and replace it with the following sentence: 'The working baseline will only be available to the TAFIM project staff.'" The goal is for the commentor to provide proposed wording that is appropriate for insertion into a TAFIM document without editing (i.e., a line-out/line-in change). The E.2 c (5), E.2 d (5), or E.2 n (5) entry in this part of the format is a discussion of the rationale for the change. The rationale may include reference material. Statements such as "industry practice" would carry less weight than specific examples. In addition, to the extent possible, citations from professional publications should be provided. A statement of the impact of the proposed change may also be included with the rationale. Finally, any other information related to improvement of the specific TAFIM document may be provided in E.2 c (6), E.2 d (6), or E.2 n (6) (i.e., the Other Comments field). However, without some degree of specificity these comments may not result in change to the document.

This page intentionally left blank.